

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC 20554**

In the Matter of

Revision of Rules and Requirements  
For Wireless Priority Service

WT Docket No. 96-86

**PETITION FOR RULEMAKING**

Pursuant to section 1.401 of the Commission's Rules and Regulations,<sup>1</sup> the National Telecommunications and Information Administration (NTIA), the President's principal adviser on domestic and international telecommunications policy, and on behalf of the Office of Emergency Communications (OEC) of the Department of Homeland Security (DHS), respectfully requests the Commission to initiate a rulemaking to update the rules and requirements for Priority Access Service (PAS), now commonly known as Wireless Priority Service (WPS).<sup>2</sup> Although WPS has evolved considerably since its creation under the PAS name in 2000, the rules governing the service have not changed since they were initially issued.<sup>3</sup>

---

<sup>1</sup> 47 C.F.R. § 1.401 (2016).

<sup>2</sup> See Matter of the Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010, *Second Report and Order*, WT Dkt. No. 96-86, 15 FCC Rcd 16720 (2000) (*Second Report*). For convenience, unless the context requires otherwise, NTIA will use the term WPS throughout this filing.

<sup>3</sup> The PAS rules were technology neutral and enabled the service to evolve with changing technologies and standards, and have accommodated Global System for Mobile Communications (GSM), Integrated Digital Enhanced Network (iDEN), Universal Mobile Telecommunications Service (UMTS), Code Division Multiple Access (CDMA) and Long Term Evolution (LTE) technologies.

This petition seeks to update those rules to reflect the current operations of WPS, the current Executive Branch governance structure for the service, and the need for more robust and reliable communications by National Security and Emergency Preparedness (NS/EP) users.

## I. INTRODUCTION

In October 1995, the National Communications System (NCS) petitioned the Commission to initiate a rulemaking proceeding to implement what the NCS termed Cellular Priority Access Service (CPAS).<sup>4</sup> CPAS was intended to allow authorized NS/EP users, during emergencies, to initiate communications whenever wireless spectrum was congested. In response, the Commission in July 2000 determined that the public interest would be served by allowing all commercial mobile radio service (CMRS) providers to offer PAS voluntarily – primarily for voice communications – to government and non-government NS/EP personnel.<sup>5</sup> “Priority access” meant that authorized NS/EP personnel could seize the next available wireless channel for emergency communications when the network is congested, although priority calls could not preempt other calls in progress.<sup>6</sup> To ensure that the new service would be compatible with any wartime priority service established by the President under section 706 of the Communications Act of 1934, and to promote compatibility between PAS in different parts of the country, the Commission required CMRS providers that choose to offer the service to do so in accordance with a set of uniform operating protocols crafted by the NCS.<sup>7</sup>

---

<sup>4</sup> Petition for Rulemaking of the National Communications System (Oct. 19, 1995) (NCS Petition), available at <https://ecfsapi.fcc.gov/file/1514910001.pdf>.

<sup>5</sup> *Second Report*, 15 FCC Rcd at 16721, ¶ 3.

<sup>6</sup> *Id.*

<sup>7</sup> *Id.* at 16733-34, ¶¶ 27-29. The operating protocols are codified in Part 64, Appendix B, of the Commission’s Rules, 47 C.F.R. Part 64, App. B, available at <https://www.gpo.gov/fdsys/pkg/CFR-2016-title47-vol3/pdf/CFR-2016-title47-vol3-part64-appB.pdf>.

The cellular network congestion in the aftermath of the terrorist attacks on September 11, 2001, led the White House to request the NCS to deploy within 60 to 90 days an “Immediate Service” using whatever network priority features were then available to make at least a rudimentary wireless priority access capability available in specific U.S. markets. Additionally, the White House called for an Initial Operational Capability that was fully compliant with the Commission’s PAS rules to be deployed no later than December 31, 2002, with a nationwide capability in place as soon as possible thereafter.<sup>8</sup> The NCS met with wireless service providers and vendors in late 2001 to identify the costs and timelines for an accelerated service implementation, as well as to develop a standards-based set of requirements for a Full Operational Capability (FOC) to be deployed nationwide by multiple service providers. Over the next several years, major service providers responded to the need by integrating PAS-compliant capabilities based on the development of PAS standards and the deployment of new network equipment.

PAS has continued to evolve since 2002, with new providers and capabilities being integrated over time.<sup>9</sup> This service currently provides end-to-end priority treatment for

---

<sup>8</sup> For additional information about the initial deployment efforts and timelines, *see* National Security Telecommunications Advisory Committee, *Wireless Task Force Report: Wireless Priority Service*, at 1 (Aug. 2002), *available at* [https://www.dhs.gov/sites/default/files/publications/Wireless%20Task%20Force%20Report\\_2002.pdf](https://www.dhs.gov/sites/default/files/publications/Wireless%20Task%20Force%20Report_2002.pdf).

<sup>9</sup> WPS achieved its FOC 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. Since then, the NCS, and later the OEC, have made a number of enhancements to WPS capabilities in the wireless technologies to keep the capabilities current while providing a high level of performance for NS/EP users. *See* DHS/OEC, *Fourth Report to the Federal Communications Commission (FCC) on Wireless Priority Service (WPS)*, at ES-1 (Oct. 7, 2014) (Fourth Report). DHS/OEC has not made the Fourth Report available to the public. Those wishing to review the Fourth Report may submit a request via email to [OEC@hq.dhs.gov](mailto:OEC@hq.dhs.gov). DHS will review all such requests and make a release determination.

authorized users, and is now referred to in both industry and government documentation as Wireless Priority Service, or WPS. While the public interest rationale for the availability of priority wireless communications in emergency situations is as compelling now as it was in 2000,<sup>10</sup> the evolution in the government structures relating to NS/EP communications, the dramatic expansion in the capacity and capabilities of wireless networks, the dramatic growth in wireless devices and the number of wireless subscribers, and the changing communications needs of NS/EP users since that time necessitate changes to the operating protocols for priority wireless communications adopted 17 years ago.

Many of the changes requested by this petition are administrative in nature – for example, to reflect shifts in the identity and/or responsibilities of the Federal agencies that oversee NS/EP communications, to address the need of more NS/EP-related entities and personnel for access to priority communications, and to recognize that priority today applies not only to network access but also to a communication’s path from end-to-end. Other changes are more substantive, such as allowing a limited set of NS/EP communications to preempt non-911 communications, and affording NS/EP users multiple ways to invoke priority treatment. Finally, we request that the Commission take steps, as it did in 2000, to remove or mitigate legal uncertainties that may inhibit CMRS providers’ willingness to make the full range of their voice, data, and video telecommunications and information services available to NS/EP personnel on a priority basis.

As more fully explained below, NTIA therefore respectfully requests that the Commission promptly initiate a rulemaking to make the revisions to Part 64, Appendix B (hereafter referred to as Appendix B throughout this filing) of its Rules set forth in Attachment 1

---

<sup>10</sup> See *Second Report*, 15 FCC Rcd at 16724-26, ¶¶ 9-12.

to this filing. None of the requirements proposed herein are intended to affect carrier obligations under existing WPS contracts (unless they are modified by agreement between the parties).

## **II. SUBSTANTIVE CHANGES TO APPENDIX B**

In this petition, we request a broad range of substantive changes and administrative and technical updates to the original WPS rules. Attachment 1 to this petition contains a “redlined” version of the rules indicating the specific changes that we propose. A number of the requested changes below will result in numerous small edits to the rules themselves, and our goal with Attachment 1 is to capture all of the changes requested below.

### **A. The Commission Should Permit a Subset of WPS Voice Calls, If Needed, to Preempt or Degrade In-Progress Public Communications, Except for Public Safety Emergency (911) Communications.**

Current WPS rules do not permit NS/EP calls to preempt other in-progress calls.<sup>11</sup> As the Executive Branch office responsible for a broad range of NS/EP communications programs (including WPS), the DHS/OEC sets the Executive Branch requirements for NS/EP communications. Since the development of the current WPS rules, and based on a number of factors (including specific Presidential policy), OEC has developed and refined requirements for WPS, including a requirement that NS/EP voice calls may degrade or preempt in-progress public communications, not including public safety emergency (911) communications.<sup>12</sup>

---

<sup>11</sup> See 47 C.F.R. Part 64, App. B, § 2.c.

<sup>12</sup> The NS/EP Priority Services Functional Requirements Specification (FRS) is a formal statement of the functional requirements for priority services developed by the OEC. The FRS serves as a basis for service contracts governing the acquisition of priority capabilities within commercial telecommunications networks. DHS/OEC has not made the FRS available to the public. Those wishing to review the FRS may submit a request via email to [OEC@hq.dhs.gov](mailto:OEC@hq.dhs.gov). DHS will review all such requests and make a release determination.

Preemption is considered a critical priority feature that will enable the highest priority NS/EP users to communicate and coordinate during emergencies, crises, or other situations where commercial networks can become congested. Current capabilities available today in leading Voice over Long Term Evolution (VoLTE) wireless networks in the United States cannot meet this need for preemption.<sup>13</sup> LTE equipment vendors, however, have built in a voice preemption capability to satisfy other countries' requirements for preemption, and U.S. service providers plan to implement these capabilities in their VoLTE services supporting WPS. OEC plans to limit the ability to preempt in-progress wireless voice calls to Priority Level 1 and 2 WPS users. Preemption will enable these higher priority users to gain access to available resources within the network, even if services to lower priority users are degraded or denied.<sup>14</sup>

Developments in standards, as well as technological advancement, now allow the delivery of differentiated mobile packet-based services (e.g., voice, data, and video telecommunications and information services) with service-specific Quality of Service (e.g., delay, jitter, loss) and fungible use of spectrum to provide a mix of service use that is optimized across numerous criteria intended to provide the best service possible in response to collective user needs and values. To meet the NS/EP needs of Priority Level 1 and 2 WPS voice users in some cases of congestion or network constraint, some wireless services may need to be

---

<sup>13</sup> For example, Long Term Evolution (LTE) networking technology does not have a queuing capability. Other built-in LTE admission control prioritization features, e.g., Automated Access Class Barring (AACB), High Priority Access (HPA), and Allocation and Retention Priority (ARP), are not effective enough for WPS calls to complete under heavy congestion. Therefore, a preemption capability is needed for NS/EP calls to gain priority access to network resources when there is contention for the resources.

<sup>14</sup> Manufacturers have already incorporated preemption capabilities, e.g., identifying preemption eligible and preemption vulnerable users, into network equipment.

dynamically degraded or preempted to permit critical NS/EP voice communications to be completed.

Granting preemption for Priority Level 1 and 2 WPS users will not significantly affect non-WPS users. As noted, preemption will apply only to WPS voice calls. Further, because Priority Level 1 and 2 is granted only to the most critical leadership of the nation, including the President, those users comprise only a small fraction of WPS users. Specifically, Priority Level 1 and 2 accounts for less than 20,000 users,<sup>15</sup> as compared to almost 396 million wireless subscriber connections in the United States.<sup>16</sup> Finally, in light of the significant increase in the capacity of VoLTE networks, the foregoing conditions assure that the preemption requested herein will be consistent with the Commission's requirement that, under WPS, "at all times a reasonable amount of CMRS spectrum is made available for public use."<sup>17</sup>

For the foregoing reasons, we request that the Commission modify Appendix B of Part 64 of its Rules to allow Priority Level 1 and 2 voice calls to be able to degrade or preempt in-progress public communications, except for public safety emergency (911) communications.

**B. The Commission Should Enable WPS Providers, at Their Option, to Give NS/EP Personnel Priority Access to and Priority Use of All Secure and Non-Secure Voice, Data, and Video Telecommunications and Information Services Available Over Their Networks.**

As noted above, the *Second Report* authorized CMRS providers to offer, on a voluntary basis, priority access to voice and low speed data services, in keeping with the capability of the CMRS networks of the time. Since 2000, the capacity and capabilities of those networks have

---

<sup>15</sup> The exact number of Priority 1 and 2 level users is not a publicly released figure, but OEC confirms that, as of the date of this filing, the number is less than 20,000.

<sup>16</sup> See CTIA, 2016 Wireless Industry Survey: Top-End Survey Results, at 2, available at <https://www.ctia.org/docs/default-source/default-document-library/annual-year-end-2016-top-line-survey-results-final.pdf?sfvrsn=2>.

<sup>17</sup> See 47 C.F.R. Part 64, App. B, § 3.e.8.

expanded immensely – due in no small part to providers’ increasing deployment of Internet Protocol (IP)-based packet switching technology – permitting wireless providers to offer a growing range of voice, data, and video telecommunications and information services, which have in turn spawned a multitude of communications applications (e.g., email, video calls, web browsing). NS/EP personnel rely on this next generation of services and applications to make and complete mission-essential communications in an efficient and effective manner.<sup>18</sup> Thus, as with preemption above, based on a number of factors, including specific Presidential policy, OEC has determined that NS/EP requirements for WPS should include priority data and video telecommunications and information services, as well as voice services.<sup>19</sup> Because of the strong public interest benefits of priority communications in emergency situations, we request that the Commission extend the concept of the voluntary offering of services from the *Second Report* to permit CMRS providers to give NS/EP personnel priority access to and use of all of their voice, data, and video telecommunications and information services.<sup>20</sup>

In 2000, the Commission recognized that CMRS providers would be unlikely to offer priority services if by so doing they risked liability for violating the Communications Act.<sup>21</sup> Because the voice services then at issue were common carrier services, the principal concern was that provision of priority services only to NS/EP personnel might violate carriers’

---

<sup>18</sup> See Communications Security, Reliability and Interoperability Council, Working Group 7, *Final Report: Planning for NS/EP Next Generation Network Priority Services During Pandemic Events 2* (Dec. 2010) (CSRIC WG7 Report), available at [https://transition.fcc.gov/pshs/docs/csric/CSRIC\\_WG7\\_Final\\_Report\\_NGN\\_Priority\\_20101216.pdf](https://transition.fcc.gov/pshs/docs/csric/CSRIC_WG7_Final_Report_NGN_Priority_20101216.pdf).

<sup>19</sup> FRS, *supra* n. 12.

<sup>20</sup> At present, OEC has no plans to fund priority services for CMRS providers other than cellular carriers.

<sup>21</sup> See *Second Report*, 15 FCC Rcd at 16722, 16730, ¶¶ 4, 22.



nondiscrimination obligations under section 202 of the Act.<sup>22</sup> To remove that potential barrier to offering such services, the Commission declared that if CMRS providers comply with the operating protocols specified in Part 64, Appendix B, they would be immune, in most circumstances, from liability under section 202.<sup>23</sup>

Allowing provision of next generation voice, data, and video telecommunications and information services on a priority basis presents similar liability concerns that could dissuade WPS providers from offering them. For example, the Commission has not ruled whether interconnected Voice over Internet Protocol (VoIP) services are “information services” or “telecommunications services.”<sup>24</sup> Thus, a CMRS provider offering priority or preemptive VoIP services only to NS/EP personnel could face the risk of litigation and potential liability for violating section 202.

Uncertainty also exists, albeit in a different way, for any broadband Internet access services (BIAS) that CMRS providers may offer as part of WPS. Although the Commission recently determined that such offerings are information services largely exempt from its

---

<sup>22</sup> *Id.* at 16730, ¶ 22.

<sup>23</sup> *See id.* at 16730-31, ¶¶ 23-24. Specifically, the Commission stated that compliance with Appendix B would render the offering of priority service *prima facie* lawful under the Act. Any complainant would “bear a heavy burden of proof to show” that such an offering was unlawfully discriminatory. *Id.* at ¶ 4.

<sup>24</sup> *See, e.g.*, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Report and Order*, 31 FCC Rcd 13911, 13925 n. 68 (2016) (“Commission has not classified interconnected VoIP service as telecommunications service or information service as those terms are defined in the Act, and we need not and do not make such a determination today.”); Numbering Policies for Modern Communications, *Report and Order*, 30 FCC Rcd 6839, 6880, ¶ 82 (2015) (in extending number portability obligations on interconnected VoIP providers, “we find it unnecessary to first determine the classification of interconnected VoIP service, and decline to do so here”).

jurisdiction,<sup>25</sup> that decision does not end federal regulatory oversight of BIAS. As the Commission notes, because most providers of fixed and wireless BIAS have committed not to block or throttle their customers' lawful Internet traffic, those commitments are now enforceable by the Federal Trade Commission (FTC) pursuant to its authority under section 5 of the Federal Trade Commission Act.<sup>26</sup> As a result, if a WPS-participant's offering of priority access to its BIAS service by NS/EP personnel could result in interference with or disruption to the traffic of other BIAS users, the provider could incur litigation costs and potential liability before the FTC.

As it did in 2000, the Commission should seek to eliminate such liability concerns for the next generation priority services that WPS providers may choose to offer. For voice services within, or potentially within, the Commission's jurisdiction – such as VoIP – the Commission should declare that if a WPS provider offers priority or preemptive access to any such service in accordance with the requirements of Part 64, Appendix B (amended as requested herein), it will be safeguarded against claims of unlawful discrimination under the Communications Act.

As for BIAS, in order to harmonize their joint authority over the providers of such services, the Commission and the FTC recently agreed, among other things, to “discuss potential investigations” and “coordinate such activities to promote consistency in law enforcement and to prevent duplicative or conflicting actions.”<sup>27</sup> The Commission should declare that if a WPS participant offers to qualified NS/EP personnel priority access to its BIAS service consistent with

---

<sup>25</sup> See Restoring Internet Freedom, *Declaratory Ruling, Report and Order, and Order*, WC Docket No. 17-108, FCC 17-166, ¶¶ 6, 26, 239 (rel. Jan. 4, 2018), available at [https://apps.fcc.gov/edocs\\_public/attachmatch/FCC-17-166A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-166A1.pdf).

<sup>26</sup> See *id.* at ¶¶ 141-42.

<sup>27</sup> Restoring Internet Freedom FCC-FTC Memorandum of Understanding, § 3 (Dec. 14, 2017), available at [https://www.ftc.gov/system/files/documents/cooperation\\_agreements/fcc\\_fcc\\_mou\\_internet\\_freedom\\_order\\_1214\\_final\\_0.pdf](https://www.ftc.gov/system/files/documents/cooperation_agreements/fcc_fcc_mou_internet_freedom_order_1214_final_0.pdf).

the requirements of Part 64, Appendix B (amended as requested herein), then the Commission would recommend that the FTC forego any action or deny any complaint under section 5. Although that recommendation would not bind the FTC,<sup>28</sup> it would likely reduce significantly the potential for an adverse FTC decision. By so doing, the FCC's declaration would reduce a legal uncertainty that may dissuade a CMRS provider from including BIAS in its WPS offerings.

**C. The Commission Should Make Changes to the WPS Description to Allow for Multiple Methods to Invoke Priority Treatment.**

In its description of WPS, Appendix B provides that authorized users can activate priority on a per call basis by dialing a specified feature code.<sup>29</sup> In all cases, obtaining WPS priority requires the invocation of WPS, as well as the deactivation of WPS (explicit or implicit) when priority is no longer to be used. For those WPS users working under emergency conditions, the requirement that WPS priority be invoked with each separate communication can hinder efficient response. If permitted, current technical standards and capabilities would allow for a variety of arrangements for WPS invocation, including "always-on" priority for selected users.

To address this concern and allow more flexibility for emergency responders, we request that the Commission modify the WPS rules to allow a variety of arrangements for WPS invocation, e.g., invoked per-application, time-limited, external signaling versus in-application signaling, and by subscription.

---

<sup>28</sup> *See id.* at § 7.

<sup>29</sup> 47 C.F.R. Part 64, Appendix B, § 2.c.

**D. The Commission Should Clarify That WPS is Intended to Address Not Only Congestion, But Also Other Conditions That Could Impair NS/EP Communications.**

In Executive Order (E.O.) 13618, the President declared that the Federal Government must have survivable, resilient, enduring, and effective communications to communicate at all times and under all circumstances to carry out its most critical and time sensitive missions.<sup>30</sup> Although network congestion is a primary cause for service degradation necessitating WPS, it is not the only condition that could imperil NS/EP mission success.

DHS has contracted for and implemented enhanced WPS solutions to address lessons learned from events that adversely affected NS/EP communications. For example, following the 2008 Los Angeles earthquake, DHS implemented Enhanced Overload Performance for Code Division Multiple Access (CDMA) wireless air interface technologies to provide: (a) priority signaling from the handset to the tower, triggered by congestion events (access), (b) priority use of network resources (transport), and (c) priority paging (egress). WPS for 4G VoLTE solutions are expected to include similar priority capabilities for access – to include automatic access class barring and the preemption capabilities available in the vendor’s equipment, and the use of many new priority capabilities for network transport and egress.

Though providers may implement WPS solutions that address congestion, these solutions may not provide the survivable priority communication solution that DHS is tasked to provide under the Executive Order.<sup>31</sup> Service providers have in some cases voluntarily provided

---

<sup>30</sup> Executive Order No. 13618, Assignment of National Security and Emergency Preparedness Communications Functions, § 1 (July 6, 2012), *available at* <https://www.gpo.gov/fdsys/pkg/CFR-2013-title3-vol1/pdf/CFR-2013-title3-vol1-eo13618.pdf>.

<sup>31</sup> Per E.O. 13618, DHS, among other things, is responsible to “incorporate, integrate, and ensure interoperability and the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability, and security to obtain, to the maximum extent practicable, the survivability of NS/EP communications . . . under all circumstances, including conditions of crisis or emergency.” *Id.* at § 5.2(b).

redundant and geographically-dispersed critical network elements, such as WPS Applications Servers and separate power grids. This need for survivability, however, is not currently addressed in the Order.

We request that the Commission amend Appendix B, as indicated in Attachment 1, so that DHS can specify requirements that ensure WPS service providers meet the survivability of NS/EP communications outlined in E.O. 13618.

**E. The Commission Should Direct WPS Providers to Provide DHS Sufficient WPS Implementation and Performance Data to Enable Assessment of the Program's Readiness, Usage, and Performance.**

On behalf of the Executive Branch, DHS is responsible for ensuring that WPS meets NS/EP needs.<sup>32</sup> To meet this obligation, DHS is required to effectively monitor WPS service, analyze the adequacy of the CMRS provider's WPS implementations, and analyze the CMRS provider's infrastructure's ability to support WPS "under all conditions." These activities require DHS to receive, store, maintain, process, and protect from disclosure (except as required by law) information from WPS providers detailing WPS usage, performance, implementation, and supporting infrastructure. In addition, DHS should also be able to assess whether WPS services are used for appropriate NS/EP purposes. To enable DHS to fulfill its responsibilities, it is valuable for DHS to receive consistent information across all WPS services providers. We thus request that the Commission specify additional responsibilities for DHS and service providers for information disclosure and protection.

In order for DHS to assure the NS/EP community of WPS acceptability, WPS service providers should be required to provide to DHS the performance and usage data necessary to

---

<sup>32</sup> *Id.* at § 5.2.

assess WPS performance and usage as a component of a nationwide NS/EP priority telecommunications service. Similarly, implementation data must be provided to enable assessing service readiness. The performance, usage, and implementation data must enable assessing WPS readiness, usage and performance at all times at all places offered, as well as for specific geographic areas and times. To ensure consistency across all WPS providers, we request that the requirement for service providers to provide this information be contained in updated rules to formalize the data exchange.

In addition to the information referenced above, we also request that WPS service providers be required to provide call information for WPS calls commonly provided in the telecommunications industry, e.g., Call Detail Records (CDR) and Operational Measurements (OM). But, because this information can arguably implicate the personal information of WPS users, it is appropriate for the Commission to require that DHS inform WPS users of this data collection, and that DHS require users, as a condition of their acceptance and use of the WPS service, to authorize service providers to release CDR information for WPS calls to DHS/OEC for the purpose of assessing readiness, usage, and performance. OEC will handle this information with the same confidentiality as Personally Identifiable Information (PII).

DHS recognizes that the CDR information collected for multi-media priority services, e.g., video, data, and information services may be different from that provided for priority voice service CDRs, because those CDRs and OMs are still to be determined. We request that the Commission adopt language in updated rules that gives the flexibility for DHS to collect this data if the technical means exist. The Commission should therefore update Appendix B, in accordance with Attachment 1, to direct WPS service providers to provide DHS requested call information, to include CDR and OM.

### III. ADDITIONAL REQUESTED CHANGES TO APPENDIX B

In addition to the most substantive changes requested above, we request that the Commission make a number of additional more administrative and technical changes to the WPS rules.

#### A. The Commission Should Change “Priority Access Service (PAS)” to “Wireless Priority Service (WPS)” to Reflect the Current Naming Convention.

The NCS originally proposed what became “PAS” to address the challenges NS/EP users faced with competition from the public for wireless radio channels during times of network congestion.<sup>33</sup> Furthermore, the NCS envisioned that PAS would eventually provide priority treatment of NS/EP communications throughout the entire end-to-end path of those communications. The CMRS standards and technologies of the day, however, did not provide the capability. To reflect the desired end-to-end nature of the service, government, industry and the White House adopted the term Wireless Priority Service in 2001.<sup>34</sup> While Appendix B refers to the service as PAS, the term WPS better reflects the service’s current requirements and capabilities. As a result, government,<sup>35</sup> industry, and users universally refer to the service as

---

<sup>33</sup> See *Second Report*, 15 FCC Rcd at 16725, ¶ 11; NCS Petition, *supra* n. 4, at 2.

<sup>34</sup> White House, Information Infrastructure Protection Assurance Group (IIPAG) Convergence Working Group, *Report on the Impact of Network Convergence on NS/EP Telecommunications: Initial Findings and FY02/FY03 Programmatic Recommendations* (July 2001). This document has not been made public. Those wishing to review the July 2001 Convergence Working Group Report may submit a request via email to [OEC@hq.dhs.gov](mailto:OEC@hq.dhs.gov). DHS will review all such requests and make a release determination.

<sup>35</sup> See, e.g., Federal Communications Commission, Wireless Priority Service (WPS), *available at* <https://www.fcc.gov/general/wireless-priority-service-wps>.

WPS. Accordingly, the Commission should change all references to PAS in Appendix B to WPS.

**B. The Commission Should Change “Radio Channels” to “Available CMRS Network Resources and Services.”**

Appendix B describes priority service as providing access to “available radio channels” during emergencies.<sup>36</sup> While the term “radio channels” has been useful since the inception of WPS, it is no longer the most accurate or descriptive term. First, broadband services in the evolving CMRS technologies are packet-oriented and no longer are appropriately considered as using radio "channels." Second, to make WPS effective for NS/EP communications under all conditions, priority is needed and is provided on network resources along the entire path of the end-to-end service. Since WPS today is an end-to-end service, it is more appropriate to describe it as priority access to and priority use of available CMRS network resources and services. The Commission should revise Appendix B accordingly, as indicated in Attachment 1.

**C. The Commission Should Update Appendix B to Reflect Current Authorities, Organizations, and Requirements Related to NS/EP Communications.**

Because Appendix B has not been changed since 2000, it no longer reflects the identities and responsibilities of the federal authorities responsible for NS/EP communications, as established by the President in E.O. 13618. Further, because Appendix B was drafted before WPS was first provided, some of its specifications do not align with practices that have developed as the service has evolved.

---

<sup>36</sup> 47 C.F.R. Part 64, App. B, § 2.c.



## **1. Role of the Executive Office of the President.**

Section 3 of Appendix B, which creates responsibilities for the various actors involved in the provision of WPS, assigns a number of responsibilities to the Executive Office of the President (EOP).<sup>37</sup> E.O. 13816, however, transferred a number of those responsibilities to DHS.<sup>38</sup> DHS, in turn, has entrusted its Office of Emergency Communications with the day-to-day administration of all of the NS/EP priority service programs to include WPS, Government Emergency Telecommunications System (GETS) and Telecommunications Service Priority (TSP).

The EOP's day-to-day responsibilities have lessened over time and now focus on establishing NS/EP requirements for national continuity policy, minimum requirements for Executive Branch continuity communications, and its role in supporting the exercise of the President's war emergency powers under section 706 of the Communications Act. Although the EOP's influence over WPS remains, E.O. 13618 assigned to DHS responsibilities for WPS that are not captured in the Commission's Rules. The Commission should therefore amend Appendix B, section 3, as in accordance with Attachment 1, to reflect the EOP's and DHS's responsibilities for WPS.

## **2. The Commission Should Replace the TSP Oversight Committee with the GETS/WPS User Council.**

Section 3 of Appendix B contemplated that the TSP System Oversight Committee would oversee the WPS system.<sup>39</sup> Today, this function is being accomplished by the GETS/WPS User Council. DHS chose to leverage the GETS/WPS User Council because it believes it better

---

<sup>37</sup> *Id.* at § 3.

<sup>38</sup> Compare E.O. 13816, § 5.2, with 47 C.F.R. Part 64, App. B, § 3.b.

<sup>39</sup> 47 C.F.R. Part 64, App. B, § 3.b.8.

serves the needs and interests of the WPS community given WPS’s operational similarity to the GETS, and in light of the council’s makeup. Membership in the GETS/WPS User Council includes GETS/WPS points of contact from Federal, state, local, and tribal government, industry, and other NS/EP organizations, as well as a representative from each of the GETS and WPS service providers. Use of the GETS/WPS User Council via its meetings provides DHS the ability to seek and receive advice on WPS program needs. We therefore request that the Commission replace references to the TSP System Oversight Committee with references to the GETS/WPS User Council.

**3. The Commission Should Modify the Responsibilities of an Authorizing Agent to Align the Rules to Reflect the Current DHS Approval Process.**

Appendix B currently specifies the responsibilities of the Federal and state “authorizing agents” that are responsible for authenticating, evaluating, and recommending to the EOP the assignment of priority levels to requesting WPS users.<sup>40</sup> The Commission’s original plan was to have a single entity in each state be a central point of contact to receive priority requests from its state users. Similarly, Federal Authorizing Agents would provide a central point of contact to receive priority requests from federal users or federally sponsored entities.<sup>41</sup> While this concept was thought to be operationally sound, in practice it did not work effectively. DHS, based on lessons learned from administering the GETS program, improved its business practices as discussed below to administer the WPS program.

DHS and WPS users (both across the Federal government and in most states) found that the requirement of a single Authorizing Agent was not practical. Many Federal agencies have

---

<sup>40</sup> See *id.* at § 2.d.1 (definition of authorizing agent).

<sup>41</sup> See *id.* at § 3.c.1.

decentralized the Authorizing Agent responsibilities and have points of contact that perform this function at multiple levels within a department or agency. Similarly, most states have multiple Authorizing Agents. This request to remove the concept of a centralized Authorizing Agent would conform to the current practice for authorizing WPS user requests/priority levels. The Commission should modify accordingly the responsibilities of an Authorizing Agent and align the rules to reflect the current DHS approval process.

**D. The Commission Should Ensure That Priority Services Serving the President Have Top Priority (Priority Level 1) Regardless of Other Priority Services Offered by WPS Providers.**

Advancements in technology and the development of standards since the inception of WPS have increased the ability of telecommunications providers to offer differentiated services with the ability to prioritize traffic flows based on an increasing number of parameters. In drafting functional requirements for Federal NS/EP priority access service (and supported by policy from the President), DHS/OEC has requested that WPS Priority Level 1 user services – those serving the President – must always have top priority regardless of any other carrier-provided priority services. Although this requirement reflects existing practice, DHS believes that it is important that the requirement that the nation’s executive leadership receive top priority be explicit and conspicuous in any revised order.<sup>42</sup> The Commission should update the description of Priority Level 1 users to make explicit that no priority treatment provided as part of any carrier service offering can exceed that offered to the President of the United States, Executive Leadership, and Policy Makers, as provided for by WPS.

---

<sup>42</sup> Leadership of OEC and the First Responder’s Network Authority (FirstNet) are collaborating to ensure that the goals of both the WPS and FirstNet can be met, and the requirement discussed here does not disrupt those goals.

**E. The Commission Should Change Descriptions of Priority Levels and Qualifying Criteria to Remove the Restriction to “Leadership and Key Personnel.”**

As originally promulgated, Appendix B indicates that WPS priority assignments are available only to key personnel and those in leadership positions, and not to all NS/EP personnel.<sup>43</sup> In large part, this limitation was put in place out of concern in the 1995 NCS petition that granting too many individuals priority access could, in and of itself, cause cellular congestion on the nation’s relatively nascent cellular telecommunications networks.<sup>44</sup> Today, wireless networks are mature, and have extensive coverage areas with abundant capacity.

Restricting WPS to leadership and key staff was shown to be problematic because it did not put priority services in the hands of individuals who required the operational capability. Lessons learned from real-world response activities clearly demonstrate that having WPS capabilities in the hands of those conducting the response activities is absolutely essential, especially given many of these responders are the ones to be operating in the areas requiring priority access. Moreover, there is now broad agreement that WPS services should be more broadly available than the original text of the rules envisioned. Specifically, DHS business practices limit the WPS user population to individuals with a bona fide NS/EP role and the ability of the infrastructure to effectively support the population of qualified NS/EP users without unduly restricting the availability of network capacity for non-WPS users.

The Commission should update the narrative for WPS Priority Levels and Qualifying Criteria to reflect current DHS business practices and not limit WPS to only key personnel and those with leadership responsibilities.

---

<sup>43</sup> 47 C.F.R. Part 64, App. B, § 5.

<sup>44</sup> See, e.g., *Second Report*, 15 FCC Rcd at 16735, ¶32.

**F. The Commission Should Update the Qualifying Criteria to Include, at a Minimum, Critical Infrastructure Protection, Financial Services, and Hospital Personnel.**

In the *Second Report*, the Commission accepted the NCS's recommendation that the WPS Qualifying Criteria and Priority Levels should follow the rules relating to the TSP system. After nearly twenty years, there is now a need to thoroughly review and update all WPS qualifying criteria and priority levels. In particular, the qualifying criteria need to be modified to accommodate three categories of NS/EP users: Critical Infrastructure Protection personnel, financial services personnel, and hospital personnel.

The emphasis in the Homeland Security Act of 2002 on critical infrastructure protection created the ability for users who perform a Critical Infrastructure Protection role to meet the qualifying criteria for WPS and this community is reflected in current DHS business practices. The Commission should modify WPS Priority Levels and Qualifying Criteria to allow entities from any of the 16 critical infrastructure sectors identified in Presidential Policy Directive (PPD)-21 to qualify for WPS Priority Level 4.<sup>45</sup>

Additionally, financial services and hospital personnel are not specifically cited in the *Second Report* and existing Appendix B. Today, however, OEC is assigning hospital personnel to WPS Priority Level 3, and financial services personnel to WPS Priority Level 4 in concert with priority level assignments established for GETS users.<sup>46</sup> The Commission should modify

---

<sup>45</sup> Presidential Policy Directive – 21, Critical Infrastructure Security and Resilience, (Feb. 12, 2013), available at <https://www.gpo.gov/fdsys/pkg/DCPD-201300092/pdf/DCPD-201300092.pdf>. The term "critical infrastructure" has the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. § 5195c(e)) (providing that "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").

<sup>46</sup> See GETS Eligibility, available at <https://www.dhs.gov/sites/default/files/publications/GETS%20eligibility%20final%20041913.pdf>.

the WPS Priority Levels and Qualifying Criteria to include these two communities of eligible WPS users.

**G. The Commission Should Allow WPS Users to Have Priority Signaling to Ensure the Network is Able to Detect WPS Invocation.**

As noted, Appendix B provides the means for NS/EP telecommunications users to obtain priority access to available radio channels when necessary to initiate emergency calls.<sup>47</sup> Lessons learned from real-world events have demonstrated that WPS effectiveness can be compromised by the effects of signaling congestion that prevent successful WPS handset network registration and service invocation.<sup>48</sup> This was first observed during the July 2008 Los Angeles earthquake. Subsequent events like the 2011 Virginia earthquake and the 2013 Boston Marathon bombing reinforced the need for WPS users to have priority signaling to ensure they could gain access to network resources to complete NS/EP calls.<sup>49</sup> In May 2010, the Commission concluded during a series of meetings with DHS that DHS's planned signaling priority enhancements to 2G/3G WPS to give WPS priority signaling access by use of an access overload class exclusive for NS/EP to the CMRS network, and the use of Advanced Signaling Priority on 4G LTE networks

---

<sup>47</sup> 47 C.F.R. Part 64, App. B, § 2.c.

<sup>48</sup> WPS data from the Los Angeles earthquake revealed that the extraordinary increase in Short Message Service (SMS) use and the growth in number of wireless handsets adversely affected NS/EP users' ability to access cellular network signaling channels. Therefore, DHS, in conjunction with major wireless providers, developed an Enhanced Overload Performance capability for select nationwide WPS providers that used CDMA. The WPS Enhanced Overload Performance capability addresses Access Channel Signaling Overload, Paging Channel Termination Overload, and Real-Time Processing Overload on the CDMA air interface. WPS Enhanced Overload Performance is based on using Access Overload Class (AOC) 12 authorized for NS/EP Mobile devices in conjunction with a standards-based load control mechanism.

<sup>49</sup> During the first 15 minutes after the Virginia earthquake, the percentage of WPS origination attempts recognized by the Mobile Switching Center was less than 15 percent for some cell sites. For the remainder of the hour after the earthquake, the percentage of recognized WPS origination attempts averaged approximately 80 percent. *See Fourth Report, supra* n. 8, at ES-23.

to give priority to WPS signaling in order to enable recognition of NS/EP invocation, were consistent with the existing rules. While the Commission concluded in these meetings that allowing users to have priority signaling was consistent with the Order and did not require Commission action,<sup>50</sup> this determination was never set out in the rules.

DHS, through its WPS service providers, has implemented signaling priority in 3G CDMA and UMTS wireless access technologies and is currently implementing advanced signaling priority in 4G VoLTE air interface technology. DHS analyses identify significant benefits of signaling priority as exemplified during the 2013 Boston Marathon bombing response.<sup>51</sup> Additionally, results of previous modeling and testing by service providers using these priority signaling features demonstrated improved performance for non-WPS calls, as well as NS/EP calls during times of network congestion.

Even though the Commission has interpreted the current rules to allow WPS priority signaling enhancements,<sup>52</sup> it should nonetheless revise Appendix B to make clear that WPS service providers can provide priority signaling to ensure the network is able to detect WPS handset network registration and service invocation.

---

<sup>50</sup> *Id.*

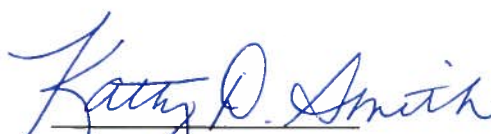
<sup>51</sup> *Id.*

<sup>52</sup> *Id.* at ES-2.

## CONCLUSION

For the foregoing reasons, NTIA respectfully requests the Commission to commence a rulemaking to update the amendments of Part 64, Appendix B of its Rules set forth in Attachment 1 of this filing.

Respectfully submitted,



Kathy D. Smith  
Chief Counsel

David J. Redl  
Assistant Secretary for  
Communications & Information

John B. Morris, Jr.  
Associate Administrator  
Evelyn Remaley  
Deputy Associate Administrator  
Shawn Cochran  
Office of Policy Analysis  
and Development

National Telecommunications  
and Information Administration  
U.S. Department of Commerce  
Room 4713  
1401 Constitution Ave, NW  
Washington, DC 20230  
(202) 482-1816

July 9, 2018



## ATTACHMENT 1

### Appendix B to Part 64 - Wireless Priority Access Service (PASWPS) for National Security and Emergency Preparedness (NSEPNS/EP)

#### 1. AUTHORITY

This appendix is issued pursuant to sections 1, 4(i), 201 through 205 and 303(r) of the Communications Act of 1934, as amended. Under these sections, the Federal Communications Commission (FCC Commission) may permit the assignment and approval of priorities for ~~access to~~ voice, data, and video telecommunications, and information services provided by commercial mobile radio service (CMRS) networks. Under section 706 of the Communications Act, this authority may be superseded by the war emergency powers of the President of the United States. This appendix provides the Commission's Order to CMRS service providers and users to comply with policies and procedures establishing the Wireless Priority Access Service (PASWPS). This appendix is intended to be read in conjunction with executive orders, regulations and procedures, and other guidance that the Executive Office of the President issues:

- (1) To implement responsibilities assigned in section 3 of this appendix, or
- (2) For use in the event this appendix is superseded by the President's emergency war powers. Together, this appendix and the regulations and ~~procedures~~ other guidance issued by the Executive Office of the President and the Department of Homeland Security (DHS) establish one uniform system of priority access wireless service both before and after invocation of the President's emergency war powers.

#### 2. BACKGROUND

- a. Purpose. This appendix establishes regulatory authorization for PASWPS to support the needs of national security and emergency preparedness (NSEPNS/EP) users of services provided by CMRS ~~users~~ licensees.
- b. Applicability. This appendix applies to the provision of PASWPS by CMRS licensees to users who qualify under the provisions of section 5 of this appendix.
- c. Description. PAS WPS provides the means for NSEPNS/EP ~~telecommunications~~ users to obtain end-to-end priority treatment on- and access to available radio channels when necessary to initiate emergency calls. It does not preempt calls in progress and ~~CMRS network resources and services.~~ WPS includes voice, data, and video telecommunications and information services, both secure and non-secure. WPS is to be used during situations when CMRS network congestion is blocking NSEP call attempts. PAS conditions in CMRS networks block NSEPNS/EP users from accessing network resources, or impair the transmission or completion of NSEPNS/EP communications. WPS is to be available to authorized NSEPNS/EP users at all times in equipped CMRS markets mobile service networks where the service CMRS provider has voluntarily decided to provide such service. Authorized users would currently activate the feature WPS on a per call basis by dialing a feature code such as \*XX. PAS priorities Vertical Service Code \*272. Enhancements to the service may allow additional forms of invocation, e.g.,

per-application. Additionally, the manner of invocation may evolve to include explicit, e.g., Vertical Service Code prefix, and implicit, e.g., secure mobile NSEPNS/EP phone or “always-on” priority. WPS users are provided priority signaling to ensure the network is able to detect WPS invocation. WPS Priority Levels 1 through 5 are reserved for qualified and authorized NSEPNS/EP users, and those users are provided access to CMRS channels/network resources before any other CMRS/public callers. Priority Level 1 & 2 WPS user voice calls can degrade or preempt in-progress public communications, except for public safety emergency (911) communications, if necessary to initiate or complete critical priority communications

d. Definitions. As used in this appendix:

1. Authorizing agent refers to a Federal ~~or~~, State, Local, Tribal, Territorial (FSLTT) or other sponsored NSEPNS/EP entity point of contact (POC) that authenticates, evaluates and makes recommendations to ~~the Executive Office of the President~~DHS regarding the assignment of WPS subscriptions and priority access service levels: (1-5).

2. Service provider means ~~an FCC~~a Commission-licensed CMRS provider, ~~that elects to participate in WPS.~~ The term does not include agents of ~~the licensed CMRS provider or resellers of CMRS service.~~such licensees.

3. Service user means an individual or organization (including a service provider) to whom or to which a WPS subscription and priority access level assignment has been made.

4. Office of Emergency Communications (OEC) refers to the DHS office that leads the Nation’s operable and interoperable public safety and NSEPNS/EP communications efforts. The OEC is the responsible U.S. Government organization for contracting for WPS with service providers.

5. The following terms have the same meaning as in Appendix A to Part 64:

(a) Assignment;

(b) Government;

(c) National Coordinating Center for Communications System; (NCC);

(d) National Coordinating Center;

~~(e) National Security and~~ Emergency Preparedness (NSEPNS/EP) Telecommunications Services (excluding the last sentence);

~~(f)~~ Reconciliation;

~~(g)~~ Revalidation;

~~(h)~~ Revision; and

~~(i)~~ Revocation.

~~e. Administration. The Executive Office of the President will administer PAS.~~

### 3. RESPONSIBILITIES

a. The *Federal Communications Commission* will provide regulatory oversight of the implementation of PASWPS, enforce PASWPS rules and regulations, and act as final authority for approval, revision, or disapproval of priority assignments by ~~the Executive Office of the President~~DHS by adjudicating disputes regarding either priority assignments or the denial thereof ~~by the Executive Office of the President~~ until superseded by the President's war emergency powers under Section 706 of the Communications Act.

b. The *Executive Office of the President (EOP)* will ~~administer the PAS system~~:

1. ~~1. Act as the final approval or denial authority for the assignment of priorities and the adjudicator of disputes during the exercise of the President's war emergency powers under section~~Section 706 of the Communications Act;
2. Assign ~~NSEPNS/EP~~ communications functions and responsibilities, for example to the Secretary of DHS, to include WPS;
3. Establish National Continuity Policy, including ~~NSEPNS/EP~~ requirements; and
4. Establish ~~m~~Minimum ~~R~~requirements for Federal Executive Branch Continuity Communications Capabilities including WPS.

c. DHS, in administering the WPS system, will:

1. Receive, process, and evaluate requests for priority actions from authorizing agents on behalf of service users or directly from service users. ~~Assign priorities or deny requests for priority using the priorities and criteria specified in section 5 of this appendix. Actions on such requests should be completed within 30 days of receipt;~~
2. ~~3. Assign priorities or deny requests for priority within 30 days of receipt using the priorities and qualifying criteria specified in section 5 of this appendix;~~
- ~~2.3.~~Convey priority assignments to the service provider and the authorizing agent;
- ~~3.4.4.~~Revise, revalidate, reconcile, and revoke priority level assignments with service users and service providers as necessary to maintain the viability of the PASWPS system;
5. ~~5. Contract, directly or indirectly, with CMRS providers for WPS service and for ~~NSEPNS/EP~~ enhancements to CMRS networks;~~
- ~~4.6.~~Maintain a database for PASWPS related information;
- ~~5.7.6.~~Issue new or revised ~~regulations,~~ procedures, and instructional material supplemental to and consistent with this appendix regarding the operation, administration, and use of PAS:WPS;
- ~~6.8.7.~~Provide training on PASWPS to affected entities and individuals;
- ~~7.9.8.~~Enlarge the role of the Government Emergency Telecommunications Service Priority System Oversight Committee (GETS)/WPS User Council to include oversight of the PASWPS system;
- ~~8.10.~~9. Report periodically to the FCC Commission on the status of PAS:WPS performance, readiness and usage; and
- ~~9.11.~~10. Disclose content of the NSEPNS/EP PASWPS database only as ~~may be~~ required by law.

ed. An Authorizing agent shall will:

1. ~~1.~~ Identify itself to DHS as an authorizing agent and its community of interest (e.g., Federal, State, Federal Agency) ~~to the EOP. State Authorizing Agents will provide a central local, tribal, territorial, or other sponsored NSEPNS/EP entity;~~
- ~~2.3.~~ ~~2.~~ Serve as a point of contact to receive priority requests from users within ~~their state. Federal Authorizing Agents will provide a central point its community of contact to receive priority requests from federal users or federally sponsored entities. interest;~~
- ~~3.4.~~ ~~2.~~ Authenticate, evaluate, and make recommendations to ~~the EOP to approve~~ DHS to establish WPS subscriptions and priority level assignment requests using the priorities and qualifying criteria specified in section 5 of this appendix. As a guide, PASWPS authorizing agents should request the lowest priority level that is applicable and the minimum number of CMRS services required to support an NSEPNS/EP function. When appropriate, the authorizing agent will recommend approval or deny requests for PASWPS.
- ~~3.4.~~ ~~3.~~ Ensure that ~~documentation information~~ is complete and accurate before forwarding it to ~~the EOP. DHS;~~
- ~~4.5.~~ ~~4.~~ Serve as a conduit for forwarding PASWPS information from ~~the EOP. DHS~~ to the service user and vice versa. Information will include PASWPS requests and assignments, training, reconciliation and revalidation notifications, and other information;
- ~~5.6.~~ ~~5.~~ Participate in annual reconciliation and revalidation of PASWPS information at the request of ~~the EOP. DHS;~~
- ~~6.7.~~ ~~6.~~ Comply with any regulations and WPS procedures supplemental to and consistent with this appendix that are issued by ~~the EOP. DHS;~~ and
- ~~7.8.~~ ~~7.~~ Disclose content of the NSEPNS/EP PASWPS database [GETS-WPS Information Distribution System (GWIDS)] only to those having a need-to-know.

~~de.~~ *Service users* will:

1. Determine the need for and request PASWPS assignments ~~in a planned process, not waiting until an emergency has occurred;~~
2. Request PASWPS assignments for the lowest applicable priority level ~~and minimum number of CMRS services~~ necessary to provide NSEPNS/EP telecommunications management and response functions during emergency/disaster situations;
3. Initiate PASWPS requests through the appropriate authorizing agent. ~~The EOP. DHS~~ will make final approval or denial of PASWPS requests and may direct service providers to remove PASWPS if appropriate. (Note: Federal, state, local, tribal, territorial and other sponsored NSEPNS/EP entities will apply for WPS through their designated authorizing agent. Other NSEPNS/EP entities will be sponsored by the Federal organization concerned with responsible for the emergency function as set forth in Executive Order 13618. If no organization is determined using these criteria, DHS/OEC will serve as the sponsoring organization. State and local government or private users will apply for PAS through their designated State government authorizing agent. Federal users will apply for PAS through their employing agency. State and local users in states where there has been no designation will be sponsored by the Federal agency concerned with the emergency function as set forth in Executive Order 12656. If no authorizing agent is determined using these criteria, the EOP will serve as the authorizing agent.);

4. Submit all ~~correspondence~~ requests for changes regarding ~~PAS~~ WPS assignments and priority levels to the authorizing agent;

5. Invoke ~~PAS~~WPS (e.g., use Vertical Service Code \*272) only when ~~CMRS congestion blocks network access and~~ the user must establish communications to fulfill an ~~NSEP~~NS/EP mission. ~~Calls should be as brief as possible so as~~ and conditions exist that impair access to afford ~~CMRS~~a service to other ~~NSEP~~ users. ~~provider's network resources.~~

6. Participate in reconciliation and revalidation of ~~PAS~~WPS information at the request of the authorizing agent or ~~the EOP~~.DHS;

7. Request discontinuance of ~~PAS~~WPS when ~~the~~their ~~NSEP~~NS/EP qualifying criteria used to obtain ~~PAS~~WPS is no longer applicable;

8. ~~Pay~~As applicable, pay service providers as billed for ~~PAS~~WPS;

9. Comply with ~~regulations and~~ procedures that are issued by ~~the EOP~~DHS which are supplemental to and consistent with this appendix; ~~and,~~

~~10. e. Service~~ Authorize service providers who offer any form of priority access service to collect and provide to DHS information regarding the user's WPS usage for ~~NSEP~~the purposes of service performance and effectiveness assessment.

~~f. Service providers will~~shall provide ~~that service~~WPS in accordance with this appendix. As ~~currently described in~~ Service providers that operate GSM and UMTS networks within their enterprise architectures will provide WPS network access priority as currently described in 3GPP TR 22.950 v6.4.0 (2005.01) and in the Priority Access and Channel Assignment (PACA) Standard (~~IS-53-A~~), ANSI/TIA 664-517-B-2007; service providers ~~will~~ that operate CDMA networks will provide WPS network access priority as currently described in 3GPP2 ~~C.S00004-A and C.S00003-D, and TIA-917-1-PACA Standard S.R0006-517-A-2007~~. Service providers will include a priority signaling capability that ensures the wireless network is able to detect WPS invocation by use of an access overload class exclusive for NS/EP as, for example, described for CDMA networks in TIA TSB-16-B-2011. Service providers that operate LTE networks will provide WPS in accordance with 3GPP TS 22.011 v13.1.0 (2014-09) and the industry-accepted technical practices for access class barring, high priority access, advanced priority, and exemption from overload controls. Service providers that operate LTE networks will use an access overload class exclusive for NS/EP as described for LTE networks in ATIS-1000061.2015. Service providers contemplating offering WPS in 5G networks – or any evolutionary/follow-on network architecture – will implement WPS in a manner that complies with DHS guidance. In addition, service providers will:

1. Provide ~~PAS~~WPS priority levels 1, 2, 3, 4, or 5 only upon receipt of an authorization from ~~the EOP~~DHS and remove ~~PAS~~WPS for specific users at the direction of ~~the EOP~~.DHS;

2. Ensure that ~~PAS~~WPS system priorities supersede any other ~~NSEP~~priority service offerings which may be ~~provided~~ offered by the service provider;

3.3. Provide DHS sufficient WPS implementation and performance data to enable DHS to assess WPS performance, readiness, and usage. (Note: DHS requires service providers to provide

information for WPS calls commonly provided in the telecommunications industry, e.g., Call Detail Records (CDR) and Operational Measurements (OM). DHS acknowledges that the CDR information collected for multi-media priority services, e.g., ~~data and video, data, and telecommunications and~~ information services may be different from that provided for priority voice CDRs, because those future multi-media CDRs and OMs are still to be determined.);

4. Designate a point of contact to coordinate with ~~the EOP~~DHS regarding ~~PAS~~WPS;

45. Participate in reconciliation and revalidation of ~~PAS~~WPS information at the request of ~~the EOP~~DHS;

56. As technically and economically feasible, provide ~~WPS~~ roaming service for users of the same grade of ~~PAS~~WPS provided to local service users;

67. Disclose content of the ~~NSEPNS/EP~~ ~~PAS~~WPS database only to those having a need-to-know ~~or who will not use the information for economic advantage;~~

78. Comply with ~~regulations~~guidance and procedures supplemental to and consistent with this appendix that are issued by ~~the EOP~~DHS;

8. ~~Insure~~9. ~~Ensure~~ that at all times a reasonable amount of ~~CMRS~~ spectrum is made available for public use; ~~and,~~

910. Notify ~~the EOP~~DHS and the service user if ~~PAS~~WPS is to be discontinued as a service.

~~f. The Telecommunications Service Priority Oversight Committee~~g. ~~The GETS/WPS User Council~~ will identify and review any systemic problems associated with ~~the PAS system~~WPS and recommend actions to correct them or prevent their recurrence.

#### **4. APPEAL**

Service users and authorizing agents may appeal any priority level assignment, denial, revision or revocation to ~~the EOP~~DHS within 30 days of notification to the service user. ~~The EOP~~ DHS will act on the appeal within 90 days of receipt. If a dispute still exists, an appeal may then be made to the ~~FCC~~Commission within 30 days of notification of ~~the EOP's~~DHS's decision. The party filing the appeal must include factual details supporting its claim and must provide a copy of the appeal to ~~the EOP~~DHS and any other party directly involved. Involved parties may file a response to the appeal made to the ~~FCC~~Commission within 20 days, and the initial filing party may file a reply within 10 days thereafter. The ~~FCC~~Commission will provide notice of its decision to the parties of record. Until a decision is made, the service will remain status quo.

#### **5. ~~PAS~~WPS PRIORITY LEVELS AND QUALIFYING CRITERIA**

The following ~~PAS~~WPS priority levels and qualifying criteria apply equally to all users and will be used as a basis for all ~~PAS~~WPS assignments. There are five levels of ~~NSEPNS/EP~~ priorities, priority one being the highest. The WPS user population should be limited only by the bona fide role of users in conduct of an ~~NSEPNS/EP~~ mission and the capacity of the infrastructure to support the population of qualified WPS users with effective service while not materially compromising the infrastructure capacity for public service. The five priority levels are:

4-1. ~~President of the United States~~, 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, and entities performing Critical Infrastructure Protection functions

5. Disaster Recovery

These priority levels were selected to meet the needs of the emergency response community and provide priority ~~access~~ 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. Priority assignments should ~~only be requested for key personnel and those individuals in national security and emergency response leadership positions.~~ PAS is not intended for use by all emergency service personnel. be allocated broadly to any users with a bona fide role in support of an ~~NSEPNS/EP~~ mission.

**A. Priority 1: President of the United States, Executive Leadership and Policy Makers.**

Priority 1 is the highest priority level in the nation, and service providers are forbidden from offering telecommunications services that prioritize user traffic ahead of Priority 1 WPS users.

Users who qualify for the President of the United States, Executive Leadership and Policy Makers priority will be assigned priority one. ~~A limited number of CMRS technicians who are essential to restoring the CMRS networks shall also receive this highest priority treatment.~~

Examples of those eligible include:

(i) The President of the United States, the Secretary of Defense, selected military leaders, and the minimum number of senior staff necessary to support these officials;

(ii) State governors, lieutenant governors, cabinet-level officials responsible for public safety and health, and the minimum number of senior staff necessary to support these officials; ~~and~~

(iii) Mayors, county commissioners, and the minimum number of senior staff to support these officials; ~~;~~ and

(iv) A limited number of technicians who are essential to restoring the mobile service networks shall also receive this highest priority treatment.

**B. Priority 2: Disaster Response/Military Command and Control**

Users who qualify for the Disaster Response/Military Command and Control priority will be assigned priority two. Individuals eligible for this priority include personnel ~~keyneeded~~ to ~~managing~~manage the initial response to an emergency at the local, state, regional and federal levels. Personnel selected for this priority should be responsible for ensuring the viability or reconstruction of the basic infrastructure in an emergency area. In addition, personnel essential to continuity of government and national security functions (such as the conduct of international affairs and intelligence activities) are also included in this priority. Examples of those eligible include:

(i) Federal emergency operations center coordinators, e.g., Manager, National Coordinating Center for ~~Telecommunications~~Communications, National Interagency Fire Center, Federal

Coordinating Officer, ~~Federal Emergency Communications~~National Continuity  
Coordinator, Director of Military Support;

(ii) State emergency ~~Services~~services director, National Guard ~~Leadership~~and Reserve,  
State and Federal Damage Assessment ~~Team Leaders~~Teams;

(iii) Federal, state and local personnel with continuity of government responsibilities;

(iv) Incident Command Center Managers, local emergency managers, other state and local  
elected public safety officials; and

(v) Federal personnel with intelligence and diplomatic responsibilities.

### **C. Priority 3: Public Health, Safety, and Law Enforcement ~~Command~~**

Users who qualify for the Public Health, Safety, and Law Enforcement ~~Command~~ priority will  
be assigned priority three. Eligible for this priority are individuals who ~~direct~~are involved in  
operations critical to life, property, and maintenance of law and order immediately following an  
event. Examples of those eligible include:

(i) Federal law enforcement ~~command~~;

(ii) State police ~~leadership~~;

(iii) Local fire and law enforcement ~~command~~;

(iv) Emergency medical service ~~leaders~~and hospital personnel;

(v) Search and rescue team ~~leaders~~members; and

(vi) Emergency communications coordinators.

### **D. Priority 4: Public Services/Utilities ~~and~~, Public Welfare and entities performing Critical Infrastructure Protection functions**

Users who qualify for the Public Services/Utilities ~~and~~, Public Welfare and Critical Infrastructure Protection priority will be assigned priority four. Eligible for this priority are  
those users whose responsibilities include managing public works ~~and~~, utility infrastructure  
damage ~~assessment~~assessments and restoration ~~efforts and~~, transportation to accomplish  
emergency response activities, or entities from any of the critical infrastructure sectors identified  
in Presidential Policy Directive – 21 whose assets, systems, and networks, whether physical or  
virtual, are considered so vital to the United States that their incapacitation or destruction would  
have a debilitating effect on security, national economic security, national public health or safety,  
or any combination thereof. Examples of those eligible include:

(i) Army Corps of Engineers ~~leadership~~personnel;

(ii) Power, water and sewage and telecommunications ~~utilities; and~~utility personnel;

(iii) Transportation ~~leadership~~and logistics personnel;

(iv) Financial services personnel

(v) Chemical sector personnel and responders; and



(vi) Defense industrial base personnel.

### **E. Priority 5: Disaster Recovery**

Users who qualify for the Disaster Recovery priority will be assigned priority five. Eligible for this priority are those individuals responsible for managing a variety of recovery operations after the initial response has been accomplished. These functions may include managing medical resources such as supplies, personnel, or patients in medical facilities. Other activities such as coordination to establish and stock shelters, to obtain detailed damage assessments, or to support ~~key~~ disaster field office personnel may be included. Examples of those eligible include:

- (i) Medical recovery operations ~~leadership~~personnel;
- (ii) Detailed damage assessment ~~leadership~~teams;
- (iii) Disaster shelter coordination and management; and
- (iv) ~~Critical Disaster~~Joint Field Office support personnel.

### **6. LIMITATIONS**

~~PAS will be assigned only to the minimum number of CMRS services required to support an NSEP function. The Executive Office of the President may also~~ DHS may establish limitations upon the relative numbers of NSEPNS/EP services that may be assigned PASWPS or the total number of PASWPS users in a serving area. These limitations will not take precedence over laws or executive orders. Limitations established shall not be exceeded.