THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

WIRELESS TASK FORCE REPORT

Wireless Priority Service

August 2002

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As part of the response to the September 11, 2001, terrorist attacks, the Office of the Manager, National Communications System (OMNCS), in concert with the White House, requested Commercial Mobile Radio Services providers to work with the OMNCS and its service integrator to implement Wireless Priority Service (WPS) on an expedited basis. During the National Security Telecommunications Advisory Committee (NSTAC) XXV Executive Breakfast, Senator Robert Bennett (R-UT) requested that the NSTAC revisit the issue of WPS and further examine obstacles to the ubiquitous rollout of WPS. In response to this charge, the NSTAC tasked the Wireless Task Force (WTF) with assessing the issues related to the ubiquitous deployment of WPS.

The WTF closely monitored the deployment of WPS, noting that the ubiquitous deployment of the program had not been achieved for a variety of operational, technical, funding, and regulatory reasons. WTF members agreed that ubiquitous, nationwide deployment of WPS would be achieved through the inclusion of all wireless technologies in the solution set, satellite back-up capabilities, and the participation of large and small wireless carriers. Members also cited inadequate Government funding, lack of liability protection for carriers, and technological limitations as additional impediments to ubiquitous rollout of WPS. Lastly, the WTF determined the need for an effective WPS outreach campaign to State and local governments, smaller wireless carriers, private sector critical infrastructure protection providers, and the general public. Providing these entities with timely and accurate information would dispel misconceptions regarding the WPS program and facilitate the inclusion of WPS in various national security and emergency preparedness (NS/EP) homeland security, contingency, and disaster recovery plans.

Based on its analysis of issues related to the ubiquitous rollout of WPS, the NSTAC offers the following recommendations:

The NSTAC recommends that the President—

- Encourage the development of WPS solutions for all wireless technologies (e.g., cellular/personal communications service, third generation networks, paging, and other wireless data services) to maximize WPS coverage, increase ubiquity, and give NS/EP users the flexibility to handle a variety of emergencies and disasters.

- Reaffirm that the Federal Communications Commission's 2nd Report and Order on Priority Access Service does extend liability protection to wireless priority solution providers equivalent to liability protection found in wireline priority communications programs.[1]

[1] See Appendix D for the minority opinion on this recommendation.

- Encourage and support adequate funding for the development and deployment of a multi-technology and multi-carrier WPS program, including a satellite backup capability to continue through WPS full operating capacity and later generations and integration with the Government Emergency Telecommunications Service (GETS).

- Direct the appropriate departments and agencies to conduct outreach and educational campaigns regarding WPS and its role in homeland security, specifically targeting—
  - State and local governments—Emphasizing the role of WPS in homeland security and the importance of expediting zoning and siting requests from wireless carriers, including the use of government sites and buildings, to increase WPS coverage and ubiquity
  - Smaller carriers—Educating them on WPS and encouraging their involvement in the program
  - Private sector critical infrastructure providers—Facilitating greater awareness of the WPS program and enabling improved contingency and disaster recovery programs
  - The general public—Detailing the benefits WPS provides for public safety and homeland security.

- Direct the National Communications System (NCS), Government agencies and departments, and organizations with NS/EP missions to implement proactive policies regarding the implementation and use of the WPS program, including—
  - Stockpiling WPS-enabled phones for large-scale distribution to NS/EP users during emergencies
  - Monitoring WPS usage following the distribution of WPS handsets to protect against fraud and abuse
  - Developing a WPS directory assistance function, enabling NS/EP users to locate one another during emergencies.

- Direct the NCS and Government agencies and departments involved in WPS planning and program management to address the technical limitations of wireless and other network technologies that may have a negative impact on the assurance, reliability, and availability of an end-to-end WPS solution. These limitations include but are not limited to—
  - Insufficient commercial capacity available to support NS/EP users
  - Technical infeasibility of offering wireless priority at the network egress within the initial operating capability time frame
  - Processing limitations of Signaling System 7 (SS7) during periods of congestion
  - Security vulnerabilities resulting from the convergence of voice and data networks and the SS7
  - Challenges associated with the integration of GETS with WPS.

1.0 INTRODUCTION AND CHARGE

Wireless Priority Service (WPS) has been under development through a joint effort by industry and Government since 1995; however, to date, the ubiquitous deployment of WPS has not been achieved for a variety of operational, technical, funding, and regulatory reasons (See Appendix C for a description of how WPS works).

As part of the response to the September 11, 2001, terrorist attacks, the Office of the Manager, National Communications System (OMNCS) in concert with the White House requested Commercial Mobile Radio Services (CMRS) providers to work with the OMNCS and its service integrator to implement WPS on an expedited basis.[1] The OMNCS' request for proposal, released on October 10, 2001, described a two-phase deployment of WPS.

The first phase of the WPS solution was dedicated to deployment in limited markets, namely Washington, DC; New York City; and Salt Lake City. This solution relied on available features, addressed only the radio access interface (i.e., not an end-to-end solution), and did not conform to the Federal Communications Commission (FCC) rule making (i.e., not on a call-by-call basis). The stated timeline for deployment was 60 days, or December 10, 2001, for the immediate solution to be deployed in Washington, DC, with New York City and Salt Lake City to follow shortly thereafter. Although the timeline for deployment was not met, a temporary WPS-like solution was devised and implemented in Salt Lake City for the 2002 Winter Olympics. The solution used a GlobalStar Satellite Service, increased trunking, and reconfigured users away from congested areas. The satellite service was supplemented by Verizon cellular service, programmed on GlobalStar handsets.

In late 2001, VoiceStream reached an agreement with the OMNCS to offer WPS pending the approval of a temporary waiver from a provision in Appendix B of the FCC's Part 64 Rules requiring authorized users to activate the feature on a per call basis. The temporary waiver was approved by the FCC on April 3, 2002, and VoiceStream implemented its WPS solution in Washington, DC, and New York City in May 2002 using a modified Enhanced Multi-Level Precedence and Preemption (eMLPP) capability, which queues the call for the next available radio resource based on the subscriber's authorized precedence level. The waiver allows all calls from a WPS subscriber's handset to be given priority treatment instead of invoking Priority Access Service (PAS) on a per call basis as required by the FCC's 2nd Report and Order (R&O) for PAS.

The second phase involves developing and deploying a near-term nationwide WPS solution. The initial development of the nationwide WPS solution included both Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA) technologies; however, the OMNCS deferred the CDMA track in anticipation of congressional funding cuts. December 2002 is the scheduled launch date for the initial operating capability (IOC), and only originating

[1] In the 2nd Report and Order (R&O) for Priority Access Service (PAS), the Federal Communications Commission (FCC) defines Commercial Mobile Radio Services (CMRS) providers as cellular licensees, broadband personal communications service (PCS) licensees, specialized mobile radio (SMR) licensees, and other mobile service providers.

national security and emergency preparedness (NS/EP) wireless traffic will have priority service. The full operating capability (FOC), scheduled for completion in late 2003, will be an end-to-end service, fully integrated with the Government Emergency Telecommunications Service (GETS) capabilities, and prioritization invoked on a call-by-call basis, complying with FCC rules.

Until nationwide deployment is fully achieved, an enhanced satellite service is scheduled to supplement the immediate solution in Washington, DC, and New York City and throughout the IOC phase. The implementation of the enhanced satellite service is largely dependent on congressional funding.

1.1 Background

During past cycles, the President's National Security Telecommunications Advisory Committee (NSTAC) has investigated the technical, administrative, and regulatory issues associated with the deployment of a nationwide WPS, including the recommendation by NSTAC's Cellular Priority Access Services (CPAS) Subgroup to the President in 1995 that the services should be made available to NS/EP users. Since the FCC's 2nd R&O for PAS was issued in July 2000, the development and deployment of WPS nationwide has been slow.

In March 2002, the NSTAC's Industry Executive Subcommittee (IES) established the Wireless Security Scoping Group (WSSG) to consider what aspects of WPS, if any, should be studied by the NSTAC. The WSSG recommended to the IES that a Wireless Task Force (WTF) be created to study issues relating to the ubiquitous rollout of WPS. In addition to analyzing the impediments to the ubiquitous rollout of WPS, the WSSG also recommended that a task force address how WPS can be promoted publicly and explore non-device specific and secure solutions for deploying WPS.

1.2 Scope of Study

The WTF tasking was limited to researching and analyzing issues related to the ubiquitous rollout of WPS with a focus to be placed on issues that the NSTAC could offer policy advice to the President regarding WPS implementation. The task force worked in conjunction with the NSTAC's Legislative and Regulatory Task Force (LRTF), which was tasked with examining the legal and regulatory aspects of WPS and the FCC's 2nd R&O. The LRTF decided to draft a joint letter with the WTF to the President addressing the interoperability of public safety communications, funding for WPS, and the ambiguity of IOC and FOC (addressed in Section 2.0 of this report).

1.3 Approach

WTF members, subject matter experts from their respective companies and associations, and Government participants contributed to this effort. Appendix A provides a list of task force members, Government personnel, and other participants. Appendix B is a briefer questionnaire prepared by the task force to assist briefers in their preparation.

2.0 ISSUES RELATED TO THE UBIQUITOUS ROLLOUT OF WPS

The WTF considered a range of issues that have contributed to the delay of WPS deployment, including operational, technical, funding, and regulatory obstacles.

The task force members considered what qualified as ubiquitous rollout. The OMNCS has defined ubiquitous rollout for the IOC as "[geographic coverage] for 75% of U.S. population (POPS) to be served by NS/EP WPS-capable infrastructure" and "a 95% or more probability that an NS/EP user making an NS/EP call in a WPS cell will have the call assigned a traffic channel within [approximately] 30 seconds." For FOC, the OMNCS has defined ubiquitous rollout as "95% of U.S. POPS to be served by WPS-capable infrastructure" and "a 90% or more probability that an NS/EP user making an NS/EP call involving originating and/or terminating wireless segments in the call path will have the call completed when all segments in the call path are NS/EP enhanced."

The task force added that the ubiquitous rollout of WPS must also include a full range of CMRS providers, and not be limited to cellular communications. For example, on September 11, 2001, many NS/EP users relied on short messaging services (SMS) and satellite communications to meet their communications needs in New York City. This reliance on alternate wireless communications capabilities was necessitated by damage to and the destruction of cell towers in lower Manhattan. The task force and the OMNCS concurred that a broader range of CMRS carriers needed to be included in WPS planning, ensuring that next generation solutions would be considered after the FOC deployment was complete.

Addressing the technology track of WPS deployment, the task force determined that, to date, WPS capabilities had been technology-specific. For example, NS/EP users require a subscription to a carrier offering WPS service. The task force discussed numerous scenarios in which a particular access technology could become unavailable, which could result in an NS/EP user not having access to priority services. Thus, the WTF concluded that WPS deployment should not follow a particular track if a ubiquitous service was the desired goal; ideally, WPS deployment requires diverse CMRS carriers and technologies. In addition, the WTF noted that other priority services, such as GETS, used a universal access number and a personal identification number (PIN) to invoke priority services. In sum, the task force agreed that solutions not dependent on specific technologies were desirable and noted that the current development scenarios for IOC and FOC were following along that path.

Among the primary concerns of wireless carriers, suppliers, manufacturers, and their agents is resolving ambiguities in the FCC's 2nd R&O on PAS. First, carriers and vendors want the FCC to ensure that IOC and any FOC solutions comply with the FCC's 2nd R&O. IOC ambiguity stems from what is considered "not unreasonable discrimination or an unreasonable preference" by offering WPS.[2] The FOC ambiguity for WPS stemmed from the fact that the R&O did not address the issue of end-to-end priority, or network egress. The task force concluded that the

[2] FCC's 2nd R&O for PAS, ¶14.

FCC's 2nd R&O for PAS extends the same protection from liability (i.e., the proscription on preferential treatment in Section 202 of the Communications Act of 1934) to carriers participating in the WPS program as carriers participating in wireline priority programs (e.g., GETS and the Telecommunications Service Priority program).

Regarding customer notification, the WTF learned that some carriers were concerned that WPS publicity may result in customers switching carriers because they fear a degradation of service and a lower rate of call completion during emergency events. Such a scenario could place carriers offering WPS to NS/EP users at a competitive disadvantage. Industry advocates have expressed concern that even the slightest increase in call blocking rates during times of emergency may cause some customers to reconsider carrier choice. The WTF determined that a ubiquitous WPS solution using a multi-carrier/multi-technology solution would alleviate this concern. The WTF also emphasized the importance of an effective WPS outreach campaign to State and local Governments and private sector critical infrastructure providers. Providing adequate information about WPS would enable these entities to include WPS capabilities in their homeland security, contingency, and disaster recovery plans.

There are also a number of issues regarding the technical feasibility of WPS implementation. The first issue is the capacity of networks to sufficiently handle NS/EP users. Considering that during most major disasters first responders are concentrated within a few cell sites, cellular networks may be unable to offer sufficient capacity to handle all wireless communications needs of the entire NS/EP user base.[3] However, additional wireless capacity can be made available relatively quickly to meet surge capacity requirements or replace damaged infrastructure, as evidenced by the wireless carriers' post-September 11, 2001, response efforts.

As determined by the WTF, other technical feasibility issues include—

- End-to-end priority: Currently, wireless priority at the network egress will not be available within the IOC time frame.

- Signaling System 7 (SS7): There are known processing limitations of SS7. During times of network congestion, these limitations could impact call completion.

- Convergence and the SS7: As a result of convergence of data and voice networks, there are certain security vulnerabilities of the SS7 that must be addressed, given the sensitivity of NS/EP communications.[4]

[3] The OMNCS and the Cellular Telecommunications & Internet Association published a study on the network capacity in large, medium, and small markets. They found in a medium-size market, such as Baton Rouge, Louisiana, the average CDMA cell site had only 54 to 108 channels. As a consequence and assuming a reasonable traffic model, the average cell site would support between 45 and 100 NS/EP users if 25 percent capacity were reserved for NS/EP users.

[4] As cited in the NSTAC's Network Security/Vulnerability Assessments Task Force Report (March 2002) and the Convergence Task Force Report (June 2001), "[Internet Protocol (IP)] networks could present those with a malicious intent a 'back door' into the control space of the [public switched telephone network], which could enable malicious activities such as insertion of false Signaling System 7 (SS7) messages."

- Integration with GETS: Currently, not all wireless carriers have the necessary trunks in place to interconnect with the existing GETS interexchange carriers.

The following sections summarize 10 issues identified by the WTF and its conclusions. In Section 2.1, impediments to the ubiquitous rollout of WPS are identified. Section 2.2 highlights issues related to how WPS should be promoted within the NS/EP community and general public with conclusions that give a general outline on how promotion should be approached. Section 2.3 offers conclusions on the technical specificity and the need for non-technology specific solutions.

2.1 What are the issues related to the ubiquitous rollout of WPS?

- **Technical limitations and security vulnerabilities of the telecommunications system (e.g., insufficient commercial capacity to support NS/EP users, technical infeasibility of offering wireless priority at the network egress within the IOC time frame, processing limitations of SS7 during congestion, security vulnerabilities resulting from the convergence of voice and data networks and the SS7[5], and the challenges associated with integrating GETS into a end-to-end WPS solution) may be an impediment to the operation of WPS.**

WPS planners and program managers need to keep these and other technical limitations in mind while further developing WPS solutions, because they threaten the assurance, reliability, and availability of an end-to-end WPS solution; these issues should be placed on a timeline to be adequately addressed by the NCS.

- **Inadequate Government funding for the WPS program has delayed the deployment of the CDMA solution and places at risk the end of year 2003 ubiquity target for FOC.**

The Government should commit to adequate funding of all wireless technology solutions (e.g., cellular/personal communications service, paging, and other wireless data services) for providing a ubiquitous FOC for WPS.

- **The administration of the WPS program is critical for managing the distribution of WPS privileges and handsets including verifying WPS users, addressing security issues, implementing fraud and abuse mechanisms, and ensuring WPS is used only for NS/EP missions.**

NCS has implemented procedures to monitor the use of WPS as required by the FCC's 2nd R&O; however, user agencies will bear much of the burden for monitoring WPS usage once phones have been distributed to their respective NS/EP personnel. In the long term, a WPS directory assistance function should be implemented as required to enable users to locate one another during emergencies.

[5] See footnote 4.

- **The Government plan to eliminate satellite backup from the WPS solution set will reduce routing and air access interface diversity. This will make the system less redundant.**

The satellite backup capability available in the immediate solution and IOC should continue to be available for FOC and later generations of WPS, because it provides a level of redundancy necessary for a program that must function during a variety of disaster and emergency situations.

- **Carriers have liability concerns regarding WPS IOC and FOC compliance with the FCC's 2nd R&O for PAS, in part caused by its technical specificity. There are also questions regarding whether carrier protection from liability extends to vendors.**

The WTF concludes that the FCC's 2nd R&O on PAS does extend the same legal liability protections to PAS providers that currently are provided to the wireline equivalent of PAS—the extremely successful GETS program. Precedent supports treating "like services alike" under the Communications Act of 1934, as amended. Creating liability parity among the "like" PAS and GETS solutions will advance participation in the PAS program and foster a more robust nationwide wireless priority solution.

2.2 How should the implementation of WPS be promoted within the NS/EP community and the general public?

- **The increased coverage necessary for carriers to deploy WPS effectively is inhibited by the inability to secure local, State, and even Federal approval for additional cell sites on or around buildings covering particularly critical areas.**

The Government should educate local, State, and Federal agencies and administrations on the necessity of WPS and the importance of enhanced coverage for effective WPS and urge them to expeditiously facilitate zoning and siting requests from wireless carriers, including the use of Government sites and buildings.

- **Aside from New York, Utah, and the Washington, DC, metropolitan area, State and local governments are largely unaware of the WPS program.**

Government agencies should coordinate with each other and with industry and academia to provide outreach to State and local officials, educating them on the WPS program and its role in homeland security. In addition, critical infrastructure protection sectors need to be made aware of the WPS program to enable improved contingency and disaster recovery programs.

- **Educating the general public on WPS places carriers offering WPS to NS/EP users at a competitive disadvantage when all carriers are not offering the service, because of consumer perceptions regarding the quality and availability of wireless service.**

The Government should educate the general public on WPS in a careful fashion, such as disseminating news releases that focus on the program's benefits for public safety. The LRTF should help discern whether carriers are required by the R&O for PAS to notify their customers of possible service degradations; such regulations would put carriers offering WPS at a competitive disadvantage, especially if WPS coverage is not ubiquitous.

- **Smaller carriers need to be made aware of the WPS program to support a broader range of NS/EP scenarios.**

Industry and Government should work together on an outreach campaign to smaller carriers to educate them on WPS and ensure their involvement.

2.3 What are non-device specific and secure solutions for deploying WPS?

- **NS/EP users are increasingly adopting wireless data applications for use in their missions; however, this raises concerns over how it may inhibit effective use of WPS over cellular networks and the lack of WPS solutions for other types of wireless networks.**

A "third generation" of WPS solutions after the deployment of FOC should extend WPS to additional CMRS devices with a focus on third generation networks and other wireless data applications. The task force did not have the opportunity to study the Department of Defense's new policy on limiting the use of wireless devices and its impact on the deployment of WPS.

- **WPS solutions are technology specific, requiring end users to subscribe to specific carriers.**

Future generations of WPS (e.g., end-to-end priority and integrated with GETS) should include solutions that use more technologies to handle a variety of emergencies and disasters. In the interim, some agencies will need to stockpile WPS-enabled phones to distribute to NS/EP users during emergencies.

3.0 RECOMMENDATIONS TO THE PRESIDENT

Based on its analysis of issues related to the ubiquitous rollout of Wireless Priority Service (WPS) and the conclusions outlined above, the National Security Telecommunications Advisory Committee (NSTAC) offers the following recommendations:

The NSTAC recommends that the President—

- Encourage the development of WPS solutions for all wireless technologies (e.g., cellular/personal communications service, third generation networks, paging, and other wireless data services) to maximize WPS coverage, increase ubiquity, and give national

security and emergency preparedness (NS/EP) users the flexibility to handle a variety of emergencies and disasters.

- Reaffirm that the Federal Communications Commission's 2nd Report and Order on Priority Access Service does extend liability protection to wireless priority solution providers equivalent to liability protection found in wireline priority communications programs.

- Encourage and support adequate funding for the development and deployment of a multi-technology and multi-carrier WPS program, including a satellite backup capability to continue through WPS full operational capability and later generations and integration with the Government Emergency Telecommunications Service (GETS).

- Direct the appropriate departments and agencies to conduct outreach and educational campaigns regarding WPS and its role in homeland security, specifically targeting—
  - State and local governments—Emphasizing the role of WPS in homeland security and the importance of expediting zoning and siting requests from wireless carriers, including the use of government sites and buildings, to increase WPS coverage and ubiquity
  - Smaller carriers—Educating them on WPS and encouraging their involvement in the program
  - Private sector critical infrastructure providers—Facilitating greater awareness of the WPS program and enabling improved contingency and disaster recovery programs
  - The general public—Detailing the benefits WPS provides for public safety and homeland security.

- Direct the National Communications System (NCS), Government agencies and departments, and organizations with NS/EP missions to implement proactive policies regarding the implementation and use of the WPS program, including—
  - Stockpiling WPS-enabled phones for large-scale distribution to NS/EP users during emergencies
  - Monitoring WPS usage following distribution of WPS handsets to protect against fraud and abuse
  - Developing a WPS directory assistance function, enabling NS/EP users to locate one another during emergencies.

- Direct the NCS and Government agencies and departments involved in WPS planning and program management to address the technical limitations of wireless and other network technologies that may have a negative impact on the assurance, reliability, and availability of an end-to-end WPS solution. These limitations include but are not limited to—
  - Insufficient commercial capacity available to support NS/EP users
  - Technical infeasibility of offering wireless priority at the network egress within the IOC time frame

- Processing limitations of Signaling System 7 (SS7) during periods of congestion
- Security vulnerabilities resulting from the convergence of voice and data networks and the SS7
- Challenges associated with the integration of GETS with WPS.

APPENDIX A

TASK FORCE MEMBERS AND OTHER PARTICIPANTS

TASK FORCE MEMBERS

Verizon Communications Inc.	Mr. James Bean, Chair
Motorola, Inc.	Mr. Ben LaPointe, Vice-Chair
SBC Communications Inc.	Ms. Rosemary Leffler, Vice-Chair
Bank of America Corporation	Mr. Jenkins Ravenel
BellSouth Corporation	Mr. Shawn Cochran
The Boeing Company	Mr. Robert Steele
Computer Sciences Corporation	Mr. Guy Copeland
Electronic Data Systems	Mr. Dale Fincke
Lockheed Martin Corporation	Ms. Jennifer Warren
Lucent Technologies	Ms. Anne Frantzen
Nortel Networks	Dr. Jack Edwards
Northrop Grumman Corporation	Mr. Scott Freber
Qwest Communications	Mr. Jon Lofstedt
Raytheon Company	Mr. Tim Bashara
Science Applications International Corporation	Mr. Hank Kluepfel
Sprint Corporation	Mr. Jim Norris
TRW Inc.	Mr. Joe Yates
WorldCom, Inc.	Mr. Thomas Gann

OTHER PARTICIPANTS

Bank of America Corporation	Mr. Sam Phillips
Cingular Wireless	Mr. Jim Bugel
Cellular Telecommunications & Internet Association	Ms. Kathryn Condello
George Washington University	Dr. Jack Oslund
Lucent Technologies	Mr. Stanley Jones
Nortel Networks	Mr. Roy McClellan
Qwest Communications	Mr. Tom Snee
Sprint Corporation	Mr. Larry Chmiel
Sprint Corporation	Ms. Carol Ross
Telecommunications Industry Association	Mr. Dan Bart
Telecommunications Industry Association	Mr. David Thompson
Verizon Communications Inc.	Mr. Andy LaChance
Verizon Wireless Inc.	Mr. Chris Carroll
VoiceStream	Mr. Gary Jones

GOVERNMENT PARTICIPANTS

OMNCS	Mr. Gary Amato
OMNCS	Mr. Vernon Mosley
OMNCS	Mr. Frank Suraci
OCS/WH	Mr. Marcus Sachs

APPENDIX B

BRIEFER QUESTIONNAIRE ON WPS

WIRELESS TASK FORCE BRIEFER QUESTIONNAIRE

The following is a list of questions prepared by the task force to assist briefers in their preparation. In the final report, the task force did not fully address every question; however, it is the intention of the task force to provide an outline of issues that will need to be addressed in the future.

The task force charge was to address the question of *what are the issues related to ubiquitous rollout of Wireless Priority Service (WPS)*. The Wireless Task Force divided the sub-questions into two categories: operational and technical.

Operational

- What are some of the potential effects (e.g., consumer perceptions, customer churn rate, etc.) on existing customer bases resulting from a carrier offering and/or activating WPS on its network?

- What is the universe of national security and emergency preparedness (NS/EP) WPS users; what safeguards can be implemented to prevent fraud and abuse, and what are the user profile factors (e.g., user type, transmission type, hold time, etc.) that may affect the performance of the WPS program?

- What are the liability concerns for carriers and vendors regarding the initial operating capability and full operating capability of WPS, especially in the context of compliance with the Federal Communications Commission's 2nd Report and Order for Priority Access Service? What if WPS fails?

- Can wireless carriers be considered as an end-to-end diverse route for NS/EP communications (i.e., more than a means of access)?

- Have wireless carriers considered the potential for density of user shift? Based on a particular event, is there a way to determine the expected number of users in a given area? Have carriers considered contingency plans in such situations, including those that involve facilities loss?

Technical

- What are the WPS network capacity issues (e.g., access at cell sites, commercial capacity in smaller markets, data transmissions, etc.)?

- What is the technical feasibility of incorporating certain capabilities (e.g., priority at network egress, internetworking and queuing at switches, interoperability with proposed State priority systems, roaming features, etc.) into WPS to provide nationwide, fully integrated WPS?

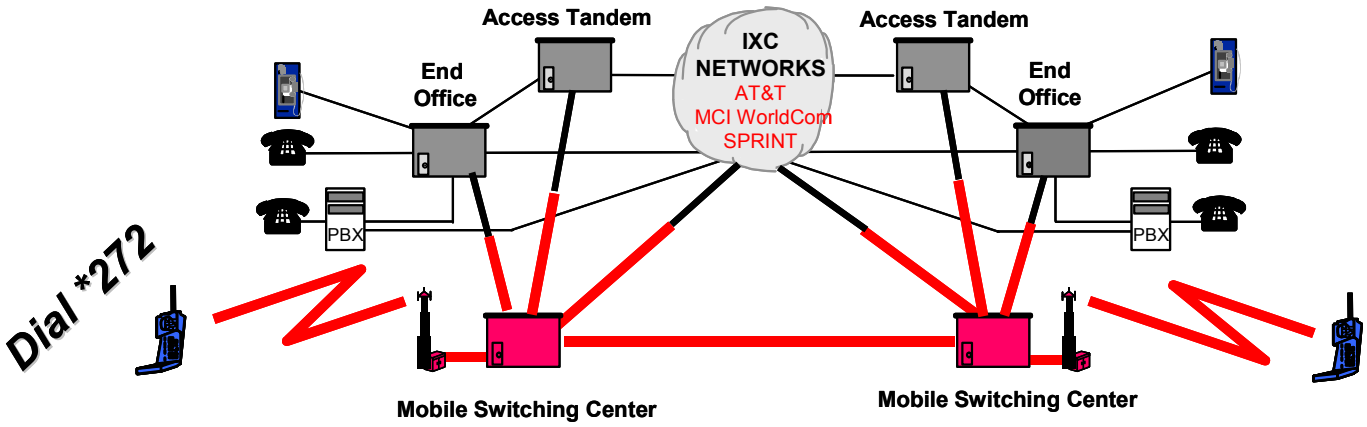
- Are there potential WPS solutions that are not device and/or technology specific?

- Given that each wireless carrier has a vision to move to third generation wireless networks, how do those technology paths mix with WPS solutions?

APPENDIX C

HOW WPS WORKS

HOW THE WPS FOC SOLUTION WORKS (AS PLANNED)



The diagram above is a representation of how the planned Wireless Priority Service (WPS) full operating capability (FOC) will work. The following is a brief description of how a WPS call will be processed.

Upon authorization from the National Communications System, the national security and emergency preparedness (NS/EP) user subscribes to a service provider that offers WPS. In the event of an emergency and network congestion, the NS/EP user invokes WPS by dialing *272 followed by the destination phone number using a WPS-enabled phone. The mobile switching center queues the call according to the user's priority level and call initiation time. When a radio traffic channel becomes available to serve a WPS request, the WPS call can proceed. The originating service provider includes the user's priority level when setting up the call through the service provider's network and any transit (e.g., interexchange carrier [IXC]) or terminating networks. The terminating network attempts to allocate a radio traffic channel before queuing the call for the next available radio traffic channel according to the call priority level and arrival time. If the queue times out before a channel becomes available, the call is dropped. The integration of WPS FOC with the Government Emergency Telecommunications Service allows priority service across all call paths; therefore, the terminating network could be either a wireless or wireline network.

APPENDIX D

MINORITY OPINION

MINORITY OPINION

The Wireless Task Force did not achieve complete consensus with respect to the recommendation to the President that states: "Reaffirm that the Federal Communications Commission's (FCC) 2nd Report and Order (R&O) on Priority Access Service (PAS) does extend liability protection to wireless priority solution providers equivalent to liability protection found in wireline priority communications programs."

Task force members agree that liability is a concern to all entities that may provide wireless priority access, but some are concerned that this recommendation, if acted upon, might result in the FCC's 2nd R&O on PAS being opened for comments and rulings by the FCC.

During the course of writing this report, the National Security Telecommunications Advisory Committee's (NSTAC) Legislative and Regulatory Task Force received comments from National Communications System (NCS) legal counsel advising it that the FCC's 2nd R&O offered sufficient liability protection. Also, the NSTAC's Industry Executive Subcommittee (IES) was briefed by the NCS with respect to meetings between the leadership of the NCS and the FCC in which the liability topic was addressed. The IES was informed that FCC leadership stated that the FCC's 2nd R&O provided liability protection to wireless priority access providers.

Reaffirmation that liability protection is extended to wireless priority solutions would help promote the ubiquitous deployment of a wireless priority service for those with a national security emergency and preparedness role. The concern among some is that the process needed to conduct this reaffirmation could ultimately be detrimental to the overall deployment of this critical national service.