

**Federal Wireless Users' Forum Workshop
October 16–18, 2002
Sands Expo and Conference Center
Las Vegas, Nevada**

Workshop Summary

Introduction

The eighteenth workshop of the Federal Wireless Users' Forum (FWUF) was held in Las Vegas, Nevada, October 16–18, 2002, at the Sands Expo and Conference Center. This workshop was co-located with the CTIA Wireless I.T. and Internet 2002 Conference, providing a special focus on wireless data technologies and services. The Federal Wireless Users' Forum, National Communications System (NCS), and the Federal Wireless Policy Committee sponsor the workshops. The objectives of the FWUF are to:

- Educate Federal Government users about wireless telecommunications and issues;
- Identify wireless telecommunications needs of Federal Government users;
- Facilitate information exchange with other user groups, standards organizations, manufacturers, and service providers, to ensure that Government user wireless needs are met, and;
- Support the interoperability of emerging wireless services and equipment through increased participation in the formulation of Federal policy, participation in wireless standards development, and other appropriate activities.

Requirements and issues identified at the workshop will be drafted and input to the Federal Wireless Policy Committee, other government decision-makers, the wireless industry, and standards organizations. A total of 189 individuals from Federal, state, and local government, equipment manufacturers, and wireless service providers attended the workshop to discuss wireless services, requirements, and issues.

The main focus of this particular workshop was changes in the Federal wireless landscape during the past year. The topics presented included a panel discussion on “The Brave New Government” – wireless for Homeland Security, Wireless Security, Wireless Priority Service, and Wireless Interoperable Communications. A dialogue session focusing on user wireless requirements and issues was held to further refine government requirements, discuss issues, and share lessons learned.

Since this workshop was co-located with the CTIA Wireless I.T. and Internet 2002 Conference, FWUF workshop attendees were able to attend all CTIA keynote addresses and also had access to the expo show floor. FWUF participants were encouraged to take advantage of the CTIA access.

Workshop Topics

The morning of the first day began with a keynote address by Michael Altschul, Senior Vice President of Policy and Administration, and General Counsel for the Cellular Telecommunications Industry Association (CTIA). Mr. Altschul discussed the role of wireless communications for federal and government users. He discussed recent litigation regarding wireless health concerns – stating that the case was dismissed because of lack of credible evidence that wireless causes brain tumors. This case is significant because it was the first opportunity for a Federal court to study current findings regarding wireless health concerns.

Since September 11, 2001, wireless has been recognized as critical infrastructure. The fractured/diverse wireless marketplace in the United States proved to be an asset, allowing for no single point of failure. Also, since September 11, 2001, wireless security is increasing in importance.

Mr. Altschul discussed the different initiatives that CTIA is involved. CTIA participates on initiatives such as the Wireless Emergency Response Team (WERT), the Network Reliability Interoperability Council, National Communications System/National Coordinating Center. CTIA also participates in efforts regarding wireless policy. Namely, CTIA has two policy arenas – spectrum and policy mandates.

After the FWUF keynote address, FWUF participants were invited to attend the CTIA keynote address. The afternoon session of the FWUF workshop featured a panel discussion on “The Brave New Government”. Government panelists discussed their views of the significance of wireless for Homeland Security.

A wireless security primer was presented on the morning of the second day. The rest of the second day was dedicated to attending the CTIA keynote and exploring the CTIA expo show floor.

The morning of the third day continued the wireless security theme along with interoperability. Afterwards, FWUF participants once again attended the CTIA keynote address. The afternoon of the third day featured a panel on wireless data and the mobile internet. A dialogue session on users issues and requirements and a discussion of future plans concluded the workshop.

Workshop Dialogue

The goals of the workshop were to identify common themes, issues, to identify and refine user wireless requirements, and enable dialogue with government and industry participants.

The Brave New Government

Brenton Greene, the Deputy Manager of NCS gave a brief history of National Security/Emergency Preparedness (NS/EP). The NCS hosts the National Security Telecommunications Advisory Committee (NSTAC), which provides industry-based

advice and expertise to the President on issues and problems related to implementing national security and emergency preparedness (NS/EP) communications policy.

Mr. Greene noted some of the NCS activities relating to priority communications services. Most notably, NCS helped to create the WERT, Wireless Priority Service (WPS), and Global Early Warning Information System (GEWIS). Wireless Priority Service will reach its final capabilities by December 2002, and will be implemented in the top 100 wireless markets by June 2004. Currently WPS is for GSM carriers only, CDMA carriers will be included in the future. GEWIS is an emergency notification system that is used to alert NS/EP personnel.

Mr. Greene explained that NCS will eventually transition to the Department of Homeland Security and when that transition occurs, NCS will ensure that there will be no gaps in operational NS/EP capabilities.

Jim Balsillic of Research In Motion (RIM) reported on the value of wireless data for government users. Information technology is a strategic enabler and gives a distinct advantage. He noted that security is a high priority for government users and that RIM has developed a Blackberry with Secure/Multipurpose Internet Mail Extensions (S/MIME) capabilities. Blackberry devices are also being developed with expanded features such as voice telephony capabilities, advanced graphics, and wireless connectivity to printers.

Rick Murphy, Co-Chair of the Public Safety Wireless Network (PSWN) Program, gave an overview of interoperability and the PSWN Program's recent efforts in assisting states improve interoperable communications. He noted that the PSWN Program is developing a "snapshot" of the state of interoperable communications across the United States. Mr. Murphy also stressed the importance of high level (state legislatures) involvement with public safety interoperable communications.

Rebel McFetridge, of the Transportation Security Administration (TSA), gave an overview of the initiatives and challenges that TSA has faced since its creation on December 31, 2001. TSA is striving towards 100% explosive detection capabilities in airports. Also, TSA is leveraging commercial wireless service offerings, taking advantage of WPS and pooled airtime plans. TSA will continue to monitor the changes in the wireless industry and use the available products and technology to support their homeland security mission.

Eric Petkus, Chief Systems Engineer of SecNet11 (Harris Corporation), presented the SecNet 11 secure WLAN solution. The SecNet 11 is a PCMCIA, Type II, 802.11b wireless LAN card. It is the first secure, encrypted, 802.11b product that is capable of Type I communications. This solution is not meant to be a replacement for wired or fiber communications, but can be used as an extension to the wired network.

Wireless Security

Tim Havighurst and Robert Nowak, both from the National Security Agency, presented a wireless security primer. Their presentation included a discussion of threats and threat mitigation strategies. Also, discussions included the need for confidentiality, data integrity, user authentication, and non-repudiation. Viruses, rogue applications, and Trojan horses were also discussed.

The primer included general guidelines for deciding what types of security are needed for particular applications. Among those guidelines are knowing what is to be protected, the value of the data to be protected, and knowing the threats that are to be mitigated. Mr. Havighurst and Mr. Nowak also discussed security policies, stating that policies exist to protect and provide guidance to prevent compromises.

Philip Maier, of Inovant, discussed the costs of risk mitigation. The cost of security is generally high, and many factors contribute to that high cost. Added costs are realized when applying security to mobile platforms. And since technology changes quickly, devices change quickly, giving the need for phased implementation strategies.

Mark Jacobs, of the NSA, provided an overview of secure wireless interoperable communications. He noted that ideal secure wireless interoperability should be end-to-end, regardless of the operating network. Further, these features should be invisible to the user. The Department of Defense (DoD) uses the Future Narrowband Digital Terminal (FNBDT) protocol. FNBDT provides Type I security. Other products exist that are not FNBDT but also provide Type I security.

Wireless Data and the Mobile Internet

John Graves, NCS Government Emergency Telecommunications Service (GETS) Program Director, discussed the GETS program and WPS. GETS is an off-the-shelf technology that provides priority service for landline telephone calls to authorized users. GETS proved its value on September 11, 2001. WPS is similar to GETS, except it is intended for wireless telecommunications networks. WPS is always on and always available for use on a call-by-call basis. WPS is expected to have full capabilities nationwide by the end of 2003.

John Limberopolous, of Sprint e-Solutions, gave an overview of Sprint's consulting platform. Sprint offers many solutions and services that are timely, robust, and stable.

Tom Soumas, of Satcom System, Inc., gave an overview of the relevance of satellite data communications within the federal user community. Satellites can be used for both voice and data communications. Homeland defense can also benefit from the use of satellite communications, gaining wide area mutual aid or command and control, redundant communications. Satellite communications give users many advantages such as access in remote areas where radio coverage is not generally available. Other advantages include worldwide coverage, secure communications, and guaranteed priority access. Further, satellites are less vulnerable to failure due to disasters compared with terrestrial based

wireless and traditional wireline services. Satellite communications is a good fit for federal users, since most applications were developed based on federal user requirements.

Tom Goodall, of Motorola, discussed the Project Greenhouse effort. Project Greenhouse provides next-generation public safety communications. It is currently operating in Pinellas County, FL. Project Greenhouse provides interoperable voice and data communications across federal, state, and local agencies. Video capabilities of Project Greenhouse are optimized for use of the wireless medium. Further, wireless automatic vehicle location is available with Project Greenhouse.

Jeff Barteo, of T-Mobile, gave an overview of T-Mobile's WPS and secure voice offerings. He mentioned that WPS was successfully deployed in New York City and Washington DC in May 2002, and will be deployed nationwide by the end of 2003. T-Mobile offers the Sectera handset that provides Type I security. The Sectera is GSM based and can roam on GSM networks in 90 countries. The Sectera handset can also work with WPS.

Workshop Conclusions

The issues listed below will be raised to the Federal Wireless Policy Committee and other government decision-making organizations.

- Wireless communications are now considered critical infrastructure. Now, more than ever, wireless is being used to support the public safety community, first responders, as well as other agencies that are charged with homeland security missions. Progress regarding government users' wireless requirements needs to continue and gain momentum.
- Wireless security continues to be on the forefront of the federal wireless user community. Users have requirements for strong encryption, authentication, access control, data integrity, and availability. Education and understanding of wireless security is the first step. Technology is continuing to progress, giving rise to more sophisticated devices with secure capabilities, but policy and education will always be critical.
- Effective interoperable communications remains an important issue to be resolved. As technology progress, federal requirements for interoperability should be addressed to ensure that interoperability is served.
- The commercial sector has recognized the importance of their offerings to federal wireless user community. Initiatives such as WPS and secure communications are being offered to federal wireless users over the commercial wireless networks. Cooperation and information sharing needs to continue between the federal wireless users and the commercial providers to ensure that requirements can be addressed.

The FWUF workshop continues to provide valuable opportunities for sharing information and partnering among government and industry participants. Many government and industry participants expressed support and appreciation for the workshop.

The next FWUF workshop is tentatively scheduled for April 8-10 in New Orleans, LA. Further information will be posted on the FWUF website as it becomes available.