Federal Wireless Users Forum

Establishment & Mission

The Federal Government recently announced the formation of a Federal Wireless Users Forum, ***FWUF***. The Forum is chaired by the Office of the Manager, National Communications System, and has a steering committee composed of representatives of eight other Federal organizations: the Department of Commerce, the Department of Defense, the Department of Justice, the General Services Administration, The National Institute of Standards and Technology, the National Security Agency, the Treasury Department, and the Chairmen of the Interagency Cellular Working Group. Objectives of the ***FWUF*** will be to:

Educate potential Government wireless users about the difficulties they may encounter.

Determine the Federal Government's user needs.

Define the most urgent issues to be resolved.

Advise vendors of Government application needs.

Facilitate the translation of Government user applications into technical applications for submission the standards bodies.

Interface with other wireless related user organizations.

The ***FWUF***'s near-term plans include; conducting wireless workshops, establishing contacts with other user groups, continuing to survey Government user needs, and working closely with industry and standards organizations.

Following are the Executive summary of the Wireless Services Task Force, letter from the President directing implementation of the reports recommendations, and attachment B of the comments made by the Manager of the National Communications System to the FCC NPRM on PCS

Towards National Security and Emergency Preparedness (NS/EP) Wireless / Low-bit-rate Bit Rate Digital Services[1]

Executive Summary

Introduction

Early in 1991 the Office of the Manager, National Communications System (OMNCS), became concerned about the possible adverse effects of certain developments in the rapidly growing and evolving wireless digital telecommunications industry regarding its ability to handle facsimile, data communications, and Secure Telephone Units (STUs). This concern is only part of a larger concern about the digital conversion problem that exist when low-bit-rate voice compression is used in the Public Switched Networks (PSNs). Working in conjunction with certain National Communications System member organizations, the OMNCS presented the issue to the Industry Executive Subcommittee (IES) of the National Security Telecommunications Advisory Committee (NSTAC). The OMNCS requested that the IES establish a task force to (1) scope the issue regarding wireless services and (2) advise the Government how to minimize any adverse impact of the emerging digital mobile communications standards and technologies on mobile National Security and Emergency Preparedness (NS/EP) users. In response the IES established a Task Force to address wireless/low-bit-rate digital services.

The Issue

The next generation wireless systems are introducing digital techniques to enhance capacity and performance. The digital voice compression techniques used in these new digital technologies provide adequate voice service, but they create a problem for NS/EP users in that they will not transparently support modem-based services such as personal computers (PCs), facsimile, and STU-IIIs currently proliferating. Supporting those current services in the emerging wireless digital networks will require special treatment by the carriers. The variety of wireless networks and the current absence of common industry-wide standards imply that future wireless digital service could require a special data device and interface for each such service on each of the different wireless networks. This situation could lead to significant NS/EP problems due to the added expense and number of devices per NS/EP user that could be required.

Based of the Task Force review of emerging wireless/low-bit-rate digital systems, the Task Force drew its conclusions and makes its recommendations to the NSTAC as pre-

[1] Report of the Wireless Services Task Force to the National Security Telecommunications Advisory Committee (NSTAC) XIII, September 5, 1991

sented below.

Conclusions

NS/EP requirements for wireless digital communications have not been clearly define to the industry. There is no Government focal point for defining such requirements. These Government NS/EP requirements need emphasis to ensure that they will be properly addressed by Government and industry.

The design of the STU-III, which uses unique analog protocols and has no digital output interfaces, is one reason for the Government's compatibility concerns.

Those portions of today's PSN involving wireless analog links support today's STU-IIIs, facsimile equipment, and modems. Some second generation systems will continue to support these devices. Third generation systems will be all-digital and may <u>not</u> support these analog devices.

There may be compatibility problems between the multitude of these analog devices and the emerging wireless digital networks. However, there are managerial approaches and economic inducements that the Government could use to mitigate these incompatibility problems; examples might be:

(1) Supply-stimulus approaches

(2) Demand-restriction approaches

(3) Legislative and regulatory-oriented approaches

Recommendations

The Government should establish a focal point, supported by NSA and NIST, to address and monitor wireless digital interface issues. The functions of this focal point should include:

Assisting industry with funding, where appropriate, to develop new or modify existing specifications for interfaces and interworking functions for mobile data communications connecting to the public switched network

Promoting the incorporation of NS/EP requirements into those industry standards under development and requesting the organization of appropriate standards bodies that do not yet exist.

Developing, where appropriate, data interface devices, protocols, and interworking functions and making these "products" available to industry.

Establishing a wireless/low-bit-rate digital communications users group, that includes both vendors and users, to exert greater NS/EP influence on the standards setting process.

In carrying out these functions, the first steps of the Government focal point should be to:

Develop in coordination with industry standards bodies, a standard interface for the Government user, encompassing both the physical layer and the control signals.

Influence the air-to-ground, mobile satellite, and personal communication network standards development groups to coordinate with the digital cellular standards community.

Organize forums with established standards groups, to include customer premise equipment providers, to address these issues.

The Government should consider a two-phased approach to making the STU devices compatible with the emerging wireless/low-bit-rate environment: (1) design a compatible digital applique' for the current STU-III; and (2) design a new generation of STUs to operate in the all-digital environment of the future.

The Government should formulate policies at a high level (such as a National Security Directive) to ensure NS/EP needs are taken into account in all wireless digital service acquisition activities. Options include:

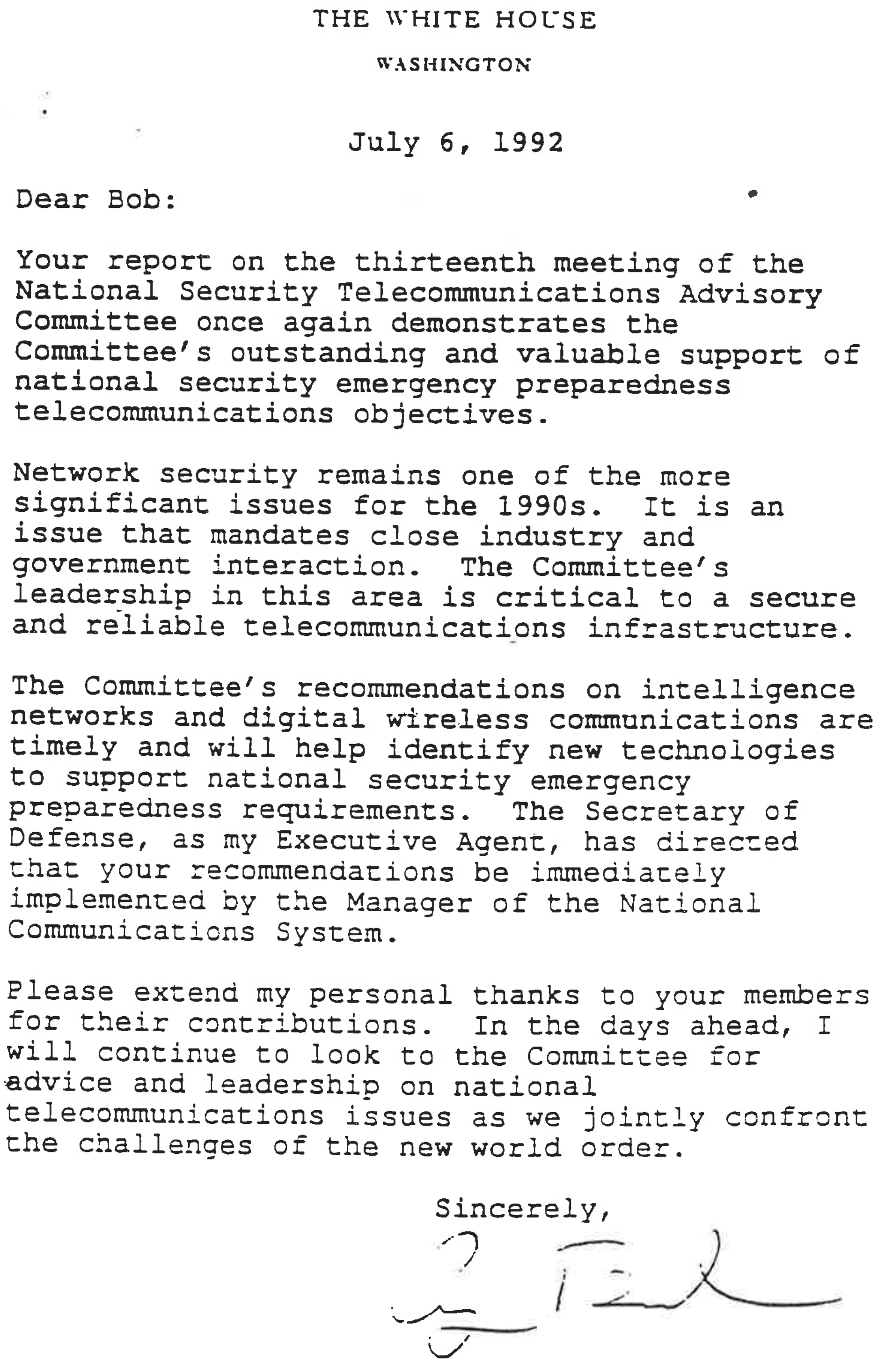
Issue directives to the NS/EP user community requiring that they subscribe only to current-data-service-compatible (STU-IIIs, facsimile, PCs) wireless/ low-bit-rate communications systems.

Consider issuing a "Notice of Inquiry" or "Request for Information" concerning industry R&D or production plans for current-data-service-compatible wireless/low-bit-rate digital communication systems.

Require standardized digital interfaces in all of its mobile telecommunications acquisition specifications, not limiting those specifications to NS/EP acquisitions only.

NSTAC member companies should wherever feasible, for purposes of National Security and Emergency Preparedness, promote the adoption of common interfaces and networking function standards across all types of wireless digital communication services, in their roles asa participants in national and international standards setting forums.

The Government should disseminate this report to appropriate standards forums within 60 days of approval by the NSTAC XIII.



THE WHITE HOUSE

WASHINGTON

July 6, 1992

Dear Bob:

Your report on the thirteenth meeting of the National Security Telecommunications Advisory Committee once again demonstrates the Committee's outstanding and valuable support of national security emergency preparedness telecommunications objectives.

Network security remains one of the more significant issues for the 1990s. It is an issue that mandates close industry and government interaction. The Committee's leadership in this area is critical to a secure and reliable telecommunications infrastructure.

The Committee's recommendations on intelligence networks and digital wireless communications are timely and will help identify new technologies to support national security emergency preparedness requirements. The Secretary of Defense, as my Executive Agent, has directed that your recommendations be immediately implemented by the Manager of the National Communications System.

Please extend my personal thanks to your members for their contributions. In the days ahead, I will continue to look to the Committee for advice and leadership on national telecommunications issues as we jointly confront the challenges of the new world order.

Sincerely,

FCC Notice of Rule Making FCC 92-333[1]

Comments Submitted by The Interagency Cellular Radio Working Group on behalf of the Federal Wireless-Services User Forum

1.0 Background

Federal government users of today's wireless communications services are especially aware of the impact Personal Communications Services (PCS) will have on their future. The availability of cost efficient and universal PCS will enhance the effectiveness and productivity of many government agencies. Such advantages however will only be realized if PCS develops to accommodate the diverse national and international missions of the federal government. Federal user requirements are similar to those of state and local governments as well as the business community and should be given serious consideration in decisions affecting the future of PCS.

The Interagency Cellular Radio Working Group (ICWG) is comprised of authorized representatives of all interested federal agencies who act on behalf of those agencies with respect to their wireless communications needs. These comments represent the views of the ICWG in its official capacity representing those agencies as cellular, and prospective PCS, customers. Therefore, the ICWG has standing as an interested party to file these comments as the authorized representative of the federal government as a cellular customer.

The Federal Wireless-Services User Forum (WUF) is group of Government wireless service users chaired by the Office of the Manager National Communications System in response to tasking by the President. Its establishment followed from recommendations of the President's National Security Telecommunications Advisory Committee in their 5 September, 1992 Report. The WUF has requested the ICWG, as the single chartered interagency government entity, to present these comments. They are put forth in the interest of an early and clear definition of the government user's need both to support the user and enhance the market and service of PCS. Many of the issues identified in the Notice of Proposed Rule Making touch on areas affecting the federal government user. The comments that follow are organized first by a summary of the federal user requirements followed by specific comments on the Notice of Proposed Rule Making.

[1] Comments of The Manager of the National Communications System, Attachment B, Pages 1-4

2.0 Federal User Requirements

The Federal User Requirements encompass a broad array of users needs in the defense and civil agencies. Wireless services provided by PCS will enhance the performance and efficiency of day to day operations of defense, law enforcement, drug enforcement, and countless other activities. These services will also play a significant role in natural disasters and crisis situations. These service requirements are common to those of the business community with few exceptions. Users require voice, data, fax, paging and imagery services for diverse applications. Security features are required in most applications. Services should appear to the user to be universally available using a common device with transparent operation. During periods of crisis it is especially important that PCS resources be available and readily configurable both nationally and internationally. These general requirements are expanded below.

2.1 Common Radio Characteristics

Ideally PCS would be supported by a single common air interface for all services nationally and internationally. While the mix of new technologies, diverse radio channels and political situations make this impractical today it is important to encourage the regulators, operators and manufacturers toward radio characteristics that can support services that are mutually compatible and can be made seamless to the user. Within the large frame work of possible access mechanisms addressed under the umbrella of PCS, some combinations of these are more important than others. The pairs of services below are thought to be those where seamless operation would be required. These paired services need not overlap.

Paired Access Mechanisms	
Satellite	Cellular
Cellular	Microcellular
Microcellular	Wireless PBX
Wireless PBX	Cordless

Seamless operation for the above paired services would imply that they would have radio characteristics that are compatible and sufficiently common that a common radio device would be practical to support both services.

2.2 Common Signalling

Common signalling mechanisms are essential if multiple access is expected under the umbrella of PCS. Where common signalling channels and protocols are not possible, automatic translation should be accomplished.

2.3 Teleservices

Independent of the wireless access mechanism a minimum set of teleservices should be available to the user. While these services might vary with the bandwidth of the access service or an intervening network, service choices and protocols should be common. These should include but are not limited to:

Voice (with a common vocoder scheme)
Asynchronous data
Synchronous Data
Group 3 and Group 4 Facsimile
STU-III encrypted voice/data
Paging
Imagery

2.4 Common User Interface

User interface for PCS devices should support a minimum set of common user interface features that will facilitate operation across the various PCS access networks and PCS devices. Examples include common key pad functions such as * and #, and common signalling such as "0perator" and "911".

2.5 Common Data Device Interface

The interface between PCS terminals and data devices should be limited to a common set of options defined by national and international standards.

2.6 Transparent Network Interworking

The teleservices identified above should be transparent to the user across a variety of wireless access networks and intervening networks. G3 facsimile, for example, should operate transparently with modem based G3 facsimile on the PSTN. Network interworking should be provided to support transparent operation of wireless PCS with the PSTN, ISDN and with Packet networks. Specifically, the federal government as a potential customer of a PCS service would require the PCS be fully interconnected with the PSTN. Without full automatic interconnection, PCS would not provide the benefit that government users would require of this service.

2.7 Security Services

Federal user requirements include a variety of security services common to the normal business user. These should be available in public PCS networks. Additional security requirements for federal users are identified as suited to private networks or supplied by the application. A Tabulation of Federal user requirements by category are shown below

FEDERAL WIRELESS REQUIREMENTS SECURITY SERVICES	Public Networks	Private Networks
Confidentiality		
Data Content	YES	YES
Signalling	NO	YES
Addressees	NO	YES
Detection	NO	YES
Identification	YES	YES
Geolocation	YES	YES
Integrity: Accidental or Malicious		
Modification	TBD	YES
Insertion	TBD	YES
Deletion	TBD	YES
Destruction	TBD	YES
Authentication		
Individual	YES	YES
Device	YES	YES
Network	NO	YES

FEDERAL WIRELESS REQUIREMENTS SECURITY SERVICES	Public Networks	Private Networks
Availability: Accidental or Malicious Denial of Service		
Survivability	YES	YES
Emergency Access	YES	YES
ECCM for malicious	NO	YES
Accountability		
Auditable	TBD	YES
Notarization	TBD	YES
Non Repudiation	TBD	YES

TBD - To Be Determined

Note: These Security Services are defined in accordance with ISO 7498-2-1988(E), Security Architecture, which is available from WUF c/o ICWG.

Comments on FCC NPRM 92-333

Leon S. Scaldeferri

Office of Information Security Research

NSA, R22
9800 Savage Rd.
Ft. Meade MD 20755-6000
(301) - 688 - 0293

FEDERAL WIRELESS USERS FORUM

MISSION

EDUCATE

DETERMINE NEEDS

DEFINE ISSUES

ADVISE VENDORS

FACILITATE

INTERFACE

FEDERAL WIRELESS REQUIREMENTS SECURITY SERVICES	Public Networks	Private (Military) Networks
Confidentiality		
Data Content	YES	YES
Signalling	NO	YES
Addressees	NO	YES
Detection	NO	YES
Identification	YES	YES
Geolocation	YES	YES
Integrity: Accidental or Malicious		
Modification	YES	YES
Insertion	YES	YES
Deletion	YES	YES
Destruction	YES	YES

FEDERAL WIRELESS REQUIREMENTS SECURITY SERVICES	Public Networks	Private (Military) Networks
Authentication		
Individual	YES	YES
Device	YES	YES
Network	NO	YES
Availability: Accidental or Malicious Denial of Service		
Survivability	YES	YES
Emergency Access	YES	YES
ECCM for malicious	NO	YES
Accountability		
Auditable	TBD	YES
Notarization	TBD	YES
Non Repudiation	TBD	YES

ISO 7498-2-1988, Security Services

802 = 802.10B, Appendix A

Security Service / Layer	1	2	3	4	5	6	7
AUTHENTICATION: (5.2.1)							
Peer Entity	*	802	ISO	ISO	*	*	ISO
Data Origin	*	802	ISO	ISO	*	*	ISO
ACCESS CONTROL: (5.2.2)	*	802	ISO	ISO	*	*	ISO
CONFIDENTIALITY: (5.2.3)							
Connection	ISO	ISO	ISO	ISO	*	ISO	ISO
Connectionless	*	ISO	ISO	ISO	*	ISO	ISO
Selective Field	*	*	*	*	*	ISO	ISO
Traffic Flow	ISO	*	ISO	*	*	*	ISO
INTEGRITY: (5.2.4)							
connection with recovery	*	*	*	ISO	*	*	ISO
connection without recovery	*	802	ISO	ISO	*	*	ISO
connectionless	*	802	ISO	ISO	*	*	ISO
ACCOUNTABILITY: (non-repudiation) (5.2.5)							
Origin	*	*	*	*	*	*	ISO
Delivery	*	*	*	*	*	*	ISO

ISO 7498-2-1988, Security Services

Security Service / Mechanism	Enc 5.3.1	DS 5.3.2	AC 5.3.3	DI 5.3.4	AE 5.3.5	TP 5.3.6	RC 5.3.7	Not 5.3.8
AUTHENTICATION: (5.2.1)								
Peer Entity	Y	Y	*	*	Y	*	*	*
Data Origin	Y	Y	*	*	*	*	*	*
ACCESS CONTROL: (5.2.2)	*	*	Y	*	*	*	*	*
CONFIDENTIALITY: (5.2.3)								
Connection/ Connectionless	Y	*	*	*	*	*	Y	*
Selective Field	Y	*	*	*	*	*	*	*
Traffic Flow	Y	*	*	*	*	Y	Y	*
INTEGRITY: (5.2.4)								
connection with recovery	Y	*	*	Y	*	*	*	*
connection without recovery	Y	*	*	Y	*	*	*	*
connectionless	Y	Y	*	Y	*	*	*	*
ACCOUNTABILITY: (non-repudiation) (5.2.5)								
Origin	*	Y	*	Y	*	*	*	Y
Delivery	*	Y	*	Y	*	*	*	Y

Threat / Security Mechanism	Enc 5.3.1	DS 5.3.2	AC 5.3.3	DI 5.3.4	AE 5.3.5	TP 5.3.6	RC 5.3.7	Not 5.3.8
MASQUERADE	*	*	*	*	Y	*	*	*
INFORMATION MODIFICATION	*	*	Y	Y	*	*	*	Y
DENIAL OF SERVICE	*	*	Y	Y	*	*	*	*
LEAKAGE OF INFORMATION	Y	*	Y	*	*	*	*	*
REPUDIATE	*	*	*	Y	Y	*	*	*
REPLAY	Y	*	*	Y	*	*	*	*

Enc - Encipherment
DS - Digital Signature
AC - Access Control
DI - Data Integrity
AE - Authentication Exchange
TP - Traffic Padding
RC - Routing Control
Not - Notarization