NRIC VII

Network Reliability and Interoperability Council VII

Issue 3 –

September 2005

FOCUS GROUP 3A

Wireless Network Reliability

Final Report

About this Document

Per the NRIC VII Council Charter, the Wireless Network Reliability Focus Group planned three issues of its report as follows, with each issue intended to make vital information available to the communications industry as it became available.

- Issue 1, Gap Analysis Report. The first Issue contains information describing the results of a gap analysis of Best Practices aimed at the reliability of wireless networks.

- Issue 2, Effectiveness Report. A second Issue was planned to include a survey of the effectiveness of the Best Practices for wireless services. This work was completed on time per the charter schedule. However, the material was not published until Issue 3.

- Issue 3, Final Report. The Final Report recommends Best Practices for wireless services providers, including the new Best Practices that particularly apply to wireless network service providers.

Each subsequent version integrates the newer material with that of the previous issue, and thus supersedes the earlier issues.

Table of Contents

1 Results in Brief

The Charter of the Seventh Council dedicated part of its focus to Network Reliability. This Network Reliability focus includes two components: Wireless Networks and Public Data Networks. This is the Final Report of the Wireless Network Reliability Focus Group and presents three deliverables.

In fulfillment of the Charter's first deliverable description, the Focus Group completed an analysis that identifies gaps in existing, documented, NRIC Best Practices for the reliability of wireless networks. Further, in fulfillment of its second prescribed deliverable, an industry survey on the effectiveness of these Best Practices was completed. Finally, to fulfill its third deliverable, the Focus Group modified existing Best Practices, and developed new Best Practices to address the specific needs of wireless networks.

The Wireless Network Reliability Focus Group reports 8 major accomplishments in this issue:

1. engagement of over 50 industry subject matter experts (Sections 2 and Section 3)
2. articulation of over 138 attributes of wireless networks
3. consideration of 285 concerns regarding wireless networks
4. formation of 8 Task Groups that provide systematic coverage of communications infrastructure elements (Section 3)
5. identification of 12 gaps in existing NRIC Best Practices (Section 3)
6. survey respondents on the effectiveness of the existing Best Practices serve over 80% of wireless subscribers in the USA (Section 3)
7. modification of 22 Best Practices to enhance their applicability to wireless networks (Section 3)
8. development of 51 new Best Practices to address wireless networks (Section 3)

1.1 Major Findings – Gap Analysis

The 12 gaps identified by this Focus Group were distributed across the infrastructure areas as follows:

Table 1.1. Distribution of Identified Gaps.

Area	Number of Gaps	Section
Environment	2	3.2.1
Hardware	0	3.2.2
Human	2	3.2.3
Network	3	3.2.4
Payload	1	3.2.5
Policy	1	3.2.6
Power	2	3.2.7
Software	1	3.2.8

In addition to these gaps the Focus Group identified potential refinements to existing Best Practices. Examples of gaps include:

Network
Air Interface Reliability
The Network Task group has identified insufficient guidance in existing Best Practices for the unique challenges related to the planning, engineering and optimization of the air interface. (Section 3.2.4)

Power
Priority Restoration of Commercial Power to Cell Sites
Critical cell sites need priority restoration of electrical power. (Section 3.2.7)

Software
Software Controls for Network Overloads
There are no NRIC Best Practices that provide guidance regarding the software implementation of overload controls so as to effectively manage traffic yet protect the reliability of the most critical nodes in a wireless network. (Section 3.2.8)

1.2 Major Findings – Effectiveness Survey

The NRIC VII Charter also directs that the Council should "…survey the wireless industry concerning the effectiveness of the Best Practices." This survey was completed on time and with several improvements over previous NRIC surveys. The following statistics summarize the survey results:

- 52% increase in the number of survey respondents (compared to NRIC V survey)
- 97% of Best Practices surveyed were rated as effective or moderately effective on average

Both the ratings and the comments provided by the respondents were studied by the Focus Group to determine what, if any, adjustments should be made to associated Best Practices. In addition to the effectiveness ratings, the Focus Group utilized comments provided by the respondents to better understand *why* a Best Practice may not be effective thus enhancing the ability to improve it.

In its analysis, the Focus Group observed that some Best Practices were identified by subject matter experts as being effective, and by other experts as being not applicable. This survey evidence further supports the principle that Best Practices are not applicable in all situations, as is stated throughout this report.

1.3 Major Findings – Best Practices Definition

Each of the Task Groups identified Best Practices by using the following three processes:

- Gap Closure Process
- Wireless Services Applicability Improvement Process
- Effectiveness Survey Process

The total number of NRIC Best Practices that were identified by the eight Task Groups is summarized in the table below (for details on the formation of the eight Task Groups refer to section 3.3.4.).

Table 1.3. Focus Group 3A Wireless Summary of Best Practice Activities.

	Gap Closure Process (12 Gaps)	Effectiveness Survey Process	Wireless Services Applicability Improvement Process	TOTAL
New Best Practices	43	0	8	**51**
Modified Best Practices	5	8	9	**22**
Deleted Best Practices	0	0	0	**0**

Section 3 provides a detailed discussion for each of the processes for each of the eight communications infrastructure areas.

Areas for Further Investigation

In addition to completing the deliverables directed by the Council Charter, the Focus Group reviewed its work to determine if there were any discoveries that went beyond its scope, but that were appropriate to present. Three such items were identified. The Policy Task Group identified the following issues: Wireless Priority Service (WPS) and emergency response to text. The Software Task Group identified handset content and third party software applications.

- **Wireless Priority Service (WPS)** - As WPS is an emerging service and not currently available for all wireless technologies, the Task Group felt it was premature to try to address this area. However, as it becomes more widely implemented, it would be of benefit to identify the industry Best Practice in its management. [Section 3.2.6.8].

- **Emergency Response to Text** – The additional functionalities provided by wireless handsets such as Short Message Service (SMS) and interactive media services create alternative means of communication to emergency response channels. Consideration should be given to advanced handset capabilities and alternatives to voice communication. . [Section 3.2.6.8].

- **Handset Content and Third Party Wireless Software Applications** - One issue that was identified as a possible gap but determined to be outside the scope of this Focus Group is the issue of manageability of third- party applications for wireless devices and handsets. Given the proliferation of content and media for wireless fixed, mobile, and handheld devices in today's voice and data networks, there are an unending number of practices that can be defined for the software development, implementation, and application management of these devices. However, in the context of Network Reliability, this Task Force determined it was appropriate to limit scope to the ability of a handset to conduct basic communications and thus did not address any gaps relative to third party wireless software applications. . [Section 3.2.8.8].

1.4 Summary of Conclusions and Recommendations

The Focus Group completed all deliverables on time and consistent with the direction of the Council Charter. This report documents highly valuable guidance for Service Providers, Network Operators, Equipment Suppliers, and Property Managers that promote the reliability for the nation's wireless networks.

Best Practice development depends on the contributions of many subject matter experts from a broad range of perspectives. The work of this focus group was effective because of the substantial time commitment by those engaged.

Going forward, industry participants are strongly encouraged to have their respective subject matter experts review these Best Practices for applicability. The NRIC web site (www.nric.org) Best Practices tools have keyword and other search capabilities that make identifying the list of applicable Best Practices to a given job function efficient. It is critical to note that Best Practices are not applicable in every situation because of multiple factors. Therefore, government entities are cautioned that mandating Best Practices could contribute to suboptimal network reliability or result in other negative consequences.

For example, Best Practices that recommend avoiding the placement of critical network facilities in high risk areas could, *if followed without appropriate consideration*, result in poor coverage. Similarly, a Best Practice that encourages deployment of certain types of back-up power, *if implemented inappropriately*, could result in a violation of local ordinances. And, likewise, a Best Practice that encourages the removal of foliage near infrastructure in some instances may result in deterioration or destruction of environmental aesthetics if proper discretion is not used.

With this understanding, the Focus Group has prepared the following recommendation for the Council to advance these Best Practices:

> **The Council recommends that the NRIC VII Wireless Network Reliability Best Practices be implemented, as appropriate, by Service Providers, Network Operators, Equipment Suppliers, and Property Managers in order to promote the reliability and robustness of the wireless networks throughout the United States.**

These Best Practices have been developed to assure optimal reliability and robustness under reasonably foreseeable circumstances. The scope of this activity also encompasses guidance that promotes the sustainability of communications networks throughout the United States, the availability of adequate communications capacity during events or periods of exceptional stress due to natural disaster, terrorist attacks or similar occurrences, and the rapid restoration of communications services in the event of widespread or major disruptions in the provision of communications services.

2 Objective, Scope, and Methodology

2.1 Objective

The Charter of the Seventh Council charged it to "…[build] on the work of the previous Councils . . . to develop Best Practices and refine or modify, as appropriate, Best Practices developed by previous Councils aimed at improving the reliability of wireless networks." Specifically, the Charter stated that "The Council shall evaluate the efficacy of all Best Practices that have been developed for the wireless industry. The Council shall perform a gap analysis to determine areas where new wireless Best Practices are needed. The Council shall survey the wireless industry concerning the effectiveness of the Best Practices. The Council shall focus on the special needs of the wireless industry and refine existing Best Practices to focus their applicability to the wireless industry." [1]

2.1.1 Mission

The Mission of the Focus Group 3A is derived directly from the NRIC VII Charter (Appendix 4). The Mission is almost verbatim from applicable sections of the Council Charter, with a few exceptions for clarification.

Focus Group 3A Mission

> **Building on the work of the previous Councils, as appropriate, this Council shall continue to develop Best Practices and refine or modify, as appropriate, Best Practices developed by previous Councils aimed at improving the reliability of wireless networks. In addition, the Council shall address the following topics in detail.**
>
> **The Council shall evaluate the efficacy of all Best Practices that have been developed for the wireless industry. The Council shall perform a gap analysis to determine areas where new wireless Best Practices are needed. The Council shall survey the wireless industry concerning the effectiveness of the Best Practices. The Council shall focus on the special needs of the wireless industry and refine existing Best Practices to focus their applicability to the wireless industry.**

[1] Council Charter, Network Reliability and Interoperability Council VII, www.nric.org.

2.1.2 Deliverables

The Focus Group 3A deliverables, as defined by the NRIC VII Charter, are:

> ***Interim Milestones***
> **By December 17, 2004, the Council shall provide a report describing the results of the gap analysis of Best Practices aimed at the reliability of wireless networks.**
>
> **By April 4, 2005, the Council shall complete its survey of the effectiveness of the Best Practices for the wireless industry.**
>
> ***Final Milestone***
> **By September 29, 2005, the Council shall provide a report recommending the Best Practices for the wireless industry including the new Best Practices that particularly apply uniquely to wireless networks.**

2.2 Scope

2.2.1 Scope Statement

This group focused on network reliability of public or commercial wireless networks serving users that have purchased a handset or device. The devices are either wireless in totality or have wireless technology as a basic element of the end service being provided (e.g., cellular, satellite, fixed wireless).

The following are outside of the scope:
Private and/or residential implementations of wireless technologies like 802.xx, Bluetooth, X10 Residential Wireless, and LMR.

2.2.2 Subject Matter

The subject matter is network reliability. Network interoperability and security are considered to the extent that they may impact network reliability.

2.2.3 Network Types

The wireless network types included in the following are Code Division Multiple Access (CDMA), Global System for Mobile Communications (GSM), integrated Digital Enhanced Network (iDEN), Advanced Mobile Phone Service (AMPS), Time Division Multiple Access (TDMA), Wireless Data, and 911 technologies.

2.2.4 Industry Roles

The scope includes Service Providers, Network Operators, Equipment Suppliers, and Property Managers of the public communications infrastructure. The following is a brief definition of the principal organizational components referred to throughout the NRIC Best Practices:[2]

[2] T1A1 Telecom Glossary: http://www.its.bldrdoc.gov/projects/telecomglossary2000

Service Providers
An organization that provides services for content providers and for users of a wireless network. The services may include access to the wireless networks. A company, organization, administration, business, etc., that sells, administers, maintains, charges for, etc., the service. The service provider may or may not be the operator of the network.

Network Operators
The wireless network operator is responsible for the development, provisioning, operations, and maintenance of real-time networking services and their corresponding networks.

Equipment Suppliers
An organization whose business is to supply wireless network operators and service providers with equipment or software required to render reliable network service.

Property Managers
The responsible party for the day-to-day operation of any facility (including rooftops and towers), usually involved at the macro level of facility operations and providing service to a communications enterprise. This responsibility may include lease management, building infrastructure operation and maintenance, landlord/tenant relations, facility standards compliance (such as OSHA), and common area maintenance and operation, which may include base building security and reception. Based on this definition, the use of "property manager" in a Best Practice would refer to the responsible operational entity, which may be the facility owner or "landlord", the majority owner of a shared facility (as in a 3DC), the owner's representative, a professional property management company, a realty management company, tenant representative (in the case of triple net or like-kind lease arrangement, a facility provider, a facility manager, or other similar positions).

Government
Government includes federal, state and local entities.

2.3 Methodology

The methodology used by this Focus Group is largely based on doing what is needed to fulfill the applicable portions of the Council Charter and by drawing from industry experience to document what works well.

The Wireless Networks Focus Group is one of two under the network reliability focus of the Seventh Council. In addition, the Seventh Council continued to pursue work addressed in previous Councils: Homeland Security and Broadband, as well as introducing a new focus on Emergency Communications Networks (Figure 2.3).

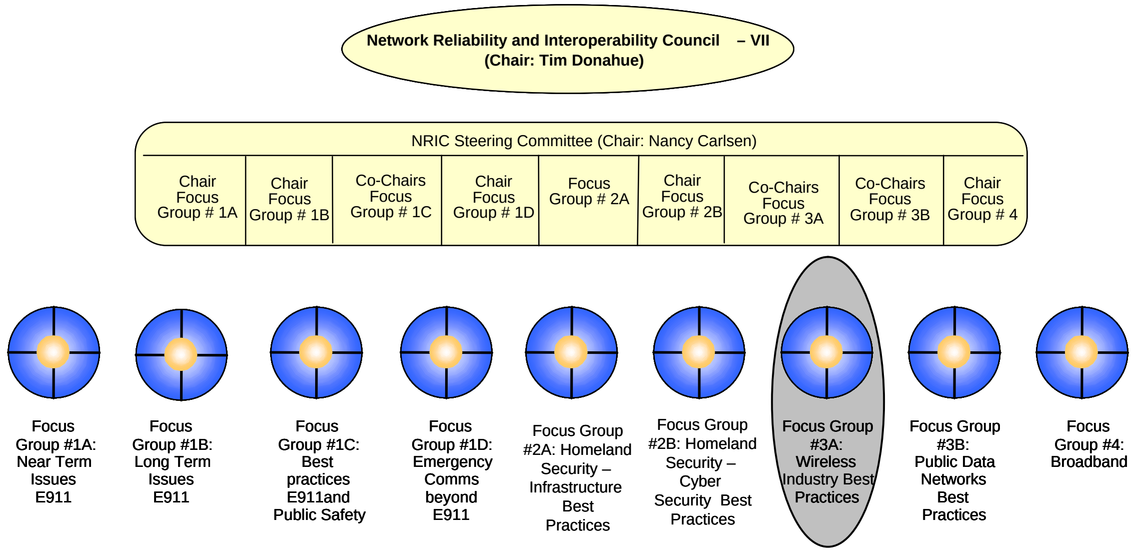

Network Reliability and Interoperability Council – VII
(Chair: Tim Donahue)
NRIC Steering Committee (Chair: Nancy Carlsen)
Chair Focus Group # 1A
Chair Focus Group # 1B
Co-Chairs Focus Group # 1C
Chair Focus Group # 1D
Focus Group # 2A
Chair Focus Group # 2B
Co-Chairs Focus Group # 3A
Co-Chairs Focus Group # 3B
Chair Focus Group # 4
Focus Group #1A: Near Term Issues E911
Focus Group #1B: Long Term Issues E911
Focus Group #1C: Best practices E911and Public Safety
Focus Group #1D: Emergency Comms beyond E911
Focus Group #2A: Homeland Security – Infrastructure Best Practices
Focus Group #2B: Homeland Security – Cyber Security Best Practices
Focus Group #3A: Wireless Industry Best Practices
Focus Group #3B: Public Data Networks Best Practices
Focus Group #4: Broadband

Figure 2.3. NRIC VII Focus Group Structure.

2.3.1 Attributes of Wireless Networks

Previous Councils have increasingly included the subject matter of wireless and then solicited the involvement of relevant expertise. For example, the Fifth Council included a Subcommittee that reviewed all existing Best Practices to determine applicability to wireless networks and services. The key words "wireless network" were used to identify applicable Best Practices; some required minor refinements of modifications.[3] The Sixth Council also included both a focus on wireless networks

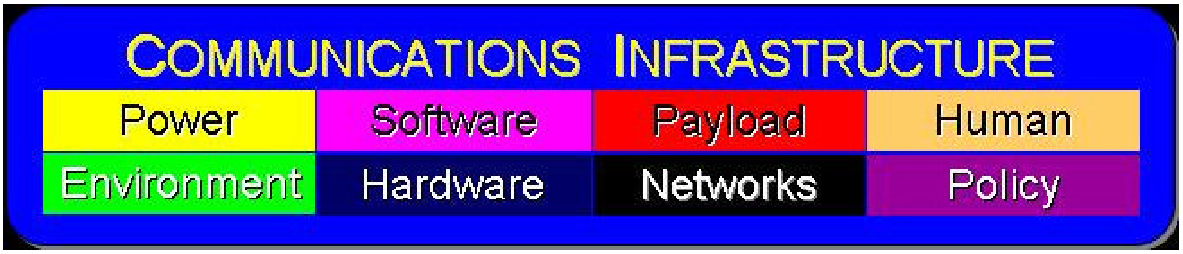
[3] NRIC V Packet Switching Network Reliability Subcommittee Final Report, January 2002, www.nric.org.

and the appropriate engagement of wireless networks expertise. However, this Seventh Council brings an even further level of attention. Recognizing the substantial work available to this Focus Group from the previous Councils, the FCC Designated Federal Officer (DFO) requested that the Focus Group ensure sufficient new rigor was brought into the process. Specifically, the DFO asked the Focus Group to “start from scratch” in its understanding of the special needs of wireless networks.

To ensure healthy rigor in understanding the special needs of wireless networks, the Focus Group assembled a list of the attributes that needed to be considered. The Focus Group generated a list of over 138 such attributes. A list of attributes of wireless networks is listed in Appendix 5.

The Focus Group then used this list of attributes along with the experience and perspectives of the membership to generate a list of 285 concerns that could affect the reliability of Wireless networks.

Each concern was then assigned to one of eight Task Groups representing the following eight areas of communications networks.



COMMUNICATIONS INFRASTRUCTURE

Power	Software	Payload	Human
Environment	Hardware	Networks	Policy

Figure 2.3.1. Eight Areas of the Communications Infrastructure.

2.3.2 Best Practices[4]

Best Practices are statements that describe the industry’s guidance to itself for the best approach to addressing a concern. NRIC Best Practices are the most authoritative list of such guidance for the communications industry. They result from unparalleled industry cooperation that engages vast expertise and considerable resources.

The implementation of specific Best Practices is intended to be voluntary. In addition, the applicability of each Best Practice for a given circumstance depends on many factors that need to be evaluated by individuals with appropriate experience and expertise in the same area the Best Practice is addressing. More information on the use of Best Practices is provided in Section 3.4.2, *Intended Use of Best Practices*. This section focuses on the factors considered in the *development* of the Best Practices. There are seven principles that are key to understanding the nature of NRIC Best Practices for the communication industry.[5]

[4] The term “Best Practices” is capitalized when referring to specific NRIC Best Practices.

[5] These principles were brought forward from the work of the NRIC V Packet Switching Network Reliability Best Practices Subcommittee and the NRIC VI Homeland Security Physical Security Focus Group.

1. “People Implement Best Practices”
The Best Practices are intended for daily use by the many thousands of individuals who support the communications infrastructure. To this end, the Best Practices address the following three values:

- applicability of Best Practices to individual job functions
- appreciation for the value of Best Practices
- accessibility to appropriate Best Practices

Even though NRIC Best Practices have been developed to be easily understood, their essence is often not immediately apparent to those who are inexperienced with the associated job functions.[6] Therefore, caution should be given to ensure that those managing Best Practices within organizations have sufficient experience.

2. Best Practices do not endorse commercial or specific "pay for" documents, products or services, but rather stress the essence of the guidance provided by such (e.g., formal quality management vs. "TL9000") practices. Helpful examples are identified in the "References Columns" available on the web site.

3. Best Practices are more effective and appropriate when they address (help prevent, mitigate, etc.) classes of problems. Detailed fixes to specific problems are not Best Practices.

4. Best Practices are already implemented by some, if not many, companies. Many fascinating and impressive ideas can be generated by the highly regarded list of organizations assembled for this effort. However, such ideas do not qualify as Best Practices if no one is “practicing them.” The recommended Best Practices provided to the industry in this document have been demonstrated to be effective, feasible and capable of being implemented.

5. Best Practices are developed by industry consensus. In particular, the parties with “skin in the game” (i.e., Service Providers, Network Operators, and Equipment Suppliers) are able to bring their expertise from across the industry to weigh in on the “best” approach to addressing a concern.

6. Best Practices are verified by a broader set of industry members – from outside the Focus Group – to ensure that those who have not been a part of the process can provide feedback. For example, an industry survey was conducted in 2005.

7. Best Practices are presented to the industry only after sufficient rigor and deliberation has warranted the inclusion of both the conceptual issue and the particular wording of the practice. Discussions among experts and stakeholders include consideration of:

- Existing implementation level of a proposed Best Practice

[6] The Keywords provide associations between job functions and Best Practices.

- Effectiveness of a proposed Best Practice
- Feasibility to implement a proposed Best Practice
- Risk not to implement a proposed Best Practice
- Alternatives to the proposed Best Practice

2.3.3 Specified Actions from the Focus Group 3A Mission Statement

The Focus Group 3A Mission Statement (Section 3.1.1) specifies 12 specific actions that are to be undertaken by the Focus Group.

1. shall continue to develop Best Practices
2. shall refine Best Practices
3. shall modify Best Practices
4. shall address the following topics [refers to items 5 through 9]:
5. shall evaluate the applicability of the Wireless Network Best Practices
6. shall perform a gap analysis to determine areas for new Wireless Network Best Practices
7. shall survey Wireless Service Providers on the efficacy of existing Best Practices.
8. shall focus on the special needs of Wireless Service Providers
9. shall refine existing Best Practices for wireless networks
10. shall provide a report on Best Practice Gaps for wireless services
11. shall complete its survey of the effectiveness of the Best Practices for wireless networks
12. shall provide a report recommending Best Practices for wireless networks

2.3.4 Participants

This section provides a brief description of the Focus Group membership's strong industry representation and activities. For approximately 25% of the organizations, their participation in this Focus Group effort was their first experience in an NRIC effort.

2.3.4.1 Industry Representation

The participants represented a balance across the industry roles (i.e., service providers, equipment suppliers, industry forums, government, others). Figure 2.3.4.1 lists the participating organizations and their representatives. In addition to the Focus Group members, additional experts were engaged from within these organizations and from other organizations to support the Task Groups described in Section 3.

The Focus Group also included a diverse array of disciplines with formal training and experience in mathematics, public policy, wireless engineering, field experience, network operations, and business management. Focus Group members referenced others within their organizations.

WIRELESS NETWORK RELIABILITY - FOCUS GROUP 3A

Co-Chair: John Quigley*, Sprint
Co-Chair: Karl F. Rauscher, Lucent Technologies Bell Labs

SERVICE PROVIDERS, NETWORK OPERATORS

ALLTEL	Steven Paton	**Qwest Wireless**	Sherman W. Phillips Stacy Hartman
AT&T	Victor DeVito*	**SBC**	John Chapa
Cingular	Jim Smith Rich Moczygemba	**Sprint**	Bill Hitchcock* Brad McManus*
Cox Communications	Mark Adams	**T-Mobile**	Tom Ellefson John Mardula*
Dobson	Scott Jones	**US Cellular**	Mike Hussey
Intelsat	Mark Neibert	**Verizon Wireless**	Chris Oberg
MCI	Mike Sheffield		
Nextel	David Proffer		

EQUIPMENT SUPPLIERS

BatteryCorp	Harold Washer	**Lucent Technologies**	Richard Krock* James P. Runyon*
Cisco Systems	Robin Roberts	**Motorola**	Lester Buczek* John Bassett*
Ericsson	Bentley Alexander*	**Nortel Networks**	Srini Anam

OTHERS

American Tower	Ted Abrams	**NCS**	Perry Fergus
ATIS	Bill Klein (A)	**NYC DOITT**	Mitchel Ahlbaum
CTIA	Rick Kemper	**SAIC**	Hank Kluepfel (A)
FCC	Jeff Goldthorp (A) Kent Nilsson (A)	**Telcordia Technologies**	Spilios Makris

*** Task Group Leaders**
A - Advisor

Figure 2.3.4.1. Wireless Networks Focus Group.

2.3.4.2 Activities

The membership was very active. Specific activities include researching issues, engaging internal and external experts, coordinating internal reviews of draft materials, completing action items and preparing for meetings. Section 2.3.5.2, *Meeting Logistics*, provides statistics on the aggregate participant-hours associated with meetings. Representatives were typically supported by several subject matter experts within their respective organizations.

2.3.5 Approach

The Focus Group's approach to fulfill its Mission was based on a new approach that would be minimally impacted by the work of previous NRIC councils. To do this, several meetings were dedicated to analysis with respect to the following areas:

The attributes of wireless networks
- Over 138 wireless network attributes were identified by this activity

The issues and problems faced by wireless networks
- Over 200 issues and problems were identified by this activity

Priority topics that the Wireless Focus Group should consider
- 12 gaps where identified (Appendix 6)

The gap closure process results
- A total of 43 New Best Practices and 5 Modifications to existing Best Practices

The Effectiveness Survey results
- A total of 8 Modifications to existing Best Practices

The services applicability improvement process
- A total of 9 New Best Practices
- A total of 8 Modifications to existing Best Practices

Using the eight dimensions of the Communications Infrastructure identified in the following Figure 2.3.5, the Focus Group formed Task Groups. The Wireless Network attributes, issues and problems, and priority topics were distributed across these Task Groups, as appropriate.

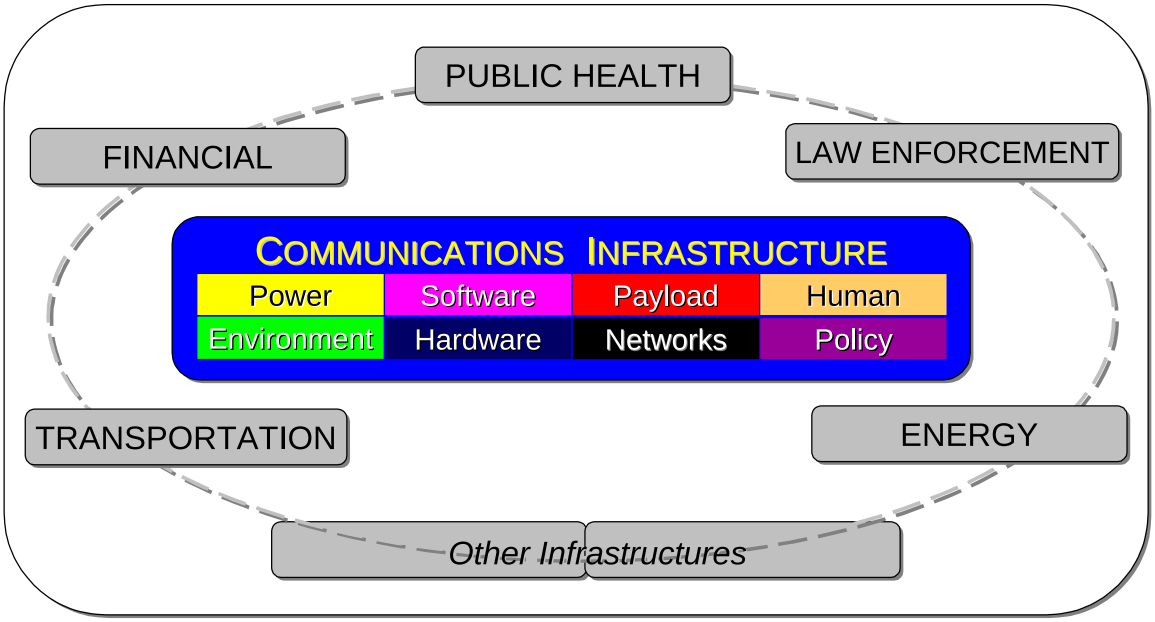


Figure 2.3.5. Communications Infrastructure.

The Task Group and Leaders are as follows:

- Environment Task Group – Victor DeVito, AT&T
- Hardware Task Group – John Bassett and Lester Buczek, Motorola
- Human Task Group – John Quigley, Sprint
- Network Task Group – Brad McManus, Sprint
- Payload Task Group – Jim Runyon, Lucent Technologies Bell Labs
- Policy Task Group – Bill Hitchcock, Sprint
- Power Task Group – John Mardula, T-Mobile and Richard Krock, Lucent Technologies Bell Labs
- Software Task Group – Bentley Alexander, Ericsson

2.3.5.1 Key Elements

There were two elements of the approach used by the Focus Group that allowed it to achieve industry-level agreements.

Consensus

A key element of the approach is that the consensus of broad industry representation articulated the Focus Group's output. This commitment to consensus greatly increased the amount of time required to agree on the Focus Group's output. However, the resulting confidence and quality are invaluable to the industry.

Protection of Sensitive Information

The Focus Group leaders encouraged all members to discuss vulnerabilities in their essence and avoid specifics, unless necessary. In addition, the Focus Group's materials and discussions were treated as confidential. A Non-Disclosure Agreement was made available by the Steering Committee Chair and signed by many of the members. This allowed participants to engage their peers with even greater protection of sensitive information.

2.3.5.2 Meeting Logistics

The Focus Group set an aggressive meeting schedule. Summary Statistics for the meetings scheduled from May 2004 through September 2005 are shown in Table 2.3.5.2.A.:

Table 2.3.5.2.A. Meeting Statistics.

Meeting Type	**Participant-Hours**
Conference Call	~500
Workshops	~2200
Total	**~2700**

In addition to the Focus Group meeting participation time, each of the eight Task Groups had numerous meetings that would account for hundreds of additional hours of meetings.

The following table provides the dates of each of the Focus Group meetings, indicates whether the meeting was a conference call or workshop and the number of participants at the meeting. Note that some meetings lasted 2 or 3 days.

Table 2.3.5.2.B. Focus Group Meetings and Participation.

2004 MEETINGS

Focus Group 3A Wireless Network Reliability

MEETING NUMBER	DATE	MEETING TYPE	PARTICIPANTS
1	May 7, 2004	Conference Call	14
2	May 21, 2004	Workshop (DC)	15
3	May 28, 2004	Conference Call	19
4	June 8, 2004	Workshop (DC)	22
	June 9, 2004	Workshop (DC)	17
5	June 28, 2004	Conference Call	20
6	July 13, 2004	Workshop (KC)	17
	July 14, 2004	Workshop (KC)	18
7	July 29, 2004	Conference Call	18
8	August 10, 2004	Workshop (IL)	15
	August 11, 2004	Workshop (IL)	16
9	August 25, 2004	Conference Call	21
10	September 20, 2004	Conference Call	22
11	October 13, 2004	Workshop (NV)	19
	October 14, 2004	Workshop (NV)	16
12	November 1, 2004	Conference Call	18
13	November 10, 2004	Workshop (DC)	12
	November 11, 2004	Workshop (DC)	14
14	November 12, 2004	Conference Call	10
15	November 15, 2004	Conference Call	9
	November 22, 2004	Power Workshop	50
16	December 14, 2004	Conference Call	17
17	December 17, 2004	Conference Call	6

2005 MEETINGS **Focus Group 3A Wireless Network Reliability**			
MEETING NUMBER	**DATE**	**MEETING TYPE**	**PARTICIPANTS**
18	January 7, 2005	Conference Call	14
19	January 14, 2005	Conference Call	17
20	January 21, 2005	Conference Call	13
21	January 28, 2005	Conference Call	15
22	February 1, 2005	Workshop (DC)	15
	February 2, 2005	Workshop (DC)	17
23	February 22, 2005	Conference Call	14
24	March 1, 2005	Workshop (DC)	13
	March 2, 2005	Workshop (DC)	14
25	March 15, 2005	Conference Call	15
26	April 6, 2005	Conference Call	17
27	April 26, 2005	Conference Call	11
28	May 17, 2005	RF Workshop (DC)	22
	May 18, 2005	RF Workshop (DC)	17
29	June 1, 2005	Conference Call	17
30	June 13, 2005	Workshop (NYC)	18
	June 14, 2005	Workshop (NYC)	18
	June 15, 2005	Workshop (NYC)	11
31	July 13, 2005	Workshop (DC)	13
	July 14, 2005	Workshop (DC)	14
32	July 28, 2005	Conference Call	13
33	August 5, 2005	Conference Call	12
34	August 10, 2005	Conference Call	16
35	August 16, 2005	Workshop (IL)	9
36	August 23, 2005	Conference Call	12

2.3.5.3 Guiding Principles for Members

The work of this Focus Group was the result of tremendous contributions from many organizations. In order to effectively work together, the team agreed to the following principles at the first face-to-face meeting:[7]

1. **The Work is Critical and Urgent**
   . . . Successful completion of our mission is vital to national security, economic stability and public safety
2. **High Quality, On-Time Deliverables that are Trustworthy and Thorough**
   . . . Fulfill applicable Charter requirements and meet the needs of the Nation
3. **Clear Objectives**
   . . . For team, and individual participants and organizations
4. **Leadership Will Pursue Consensus of Team**
   . . . Also needs to set pace & guide fulfillment of charter
5. **Follow a Scientific Approach, Not Merely Collect Subjective Opinions**
   . . . Be objective and practice a disciplined methodology
6. **Capture Every Good Idea**
   . . . Welcome new and different perspectives for consideration
7. **Respect for Individuals**
   . . . Open and honest interactions

2.3.6 Coordination with Other Stakeholders

In order to avoid unnecessary duplication of effort and to better realize synergies, the leaders of NRIC and other key entities have appropriately agreed to coordinate their activities. Government and industry stakeholders include the following organizations and their constituents:

- Alliance for Industry Solutions (ATIS)
  - Network Reliability Steering Committee (NRSC)
- American National Standards Institute (ANSI)
- Cellular Telecommunications and Internet Association (CTIA)
- Institute of Electrical and Electronics Engineers (IEEE)
  - Communications Society (COMSOC)
  - Technical Committee on Communications Quality & Reliability (CQR)
- International Engineering Consortium (IEC)
- Internet Engineering Task Force (IETF)
- International Telecommunications Union (ITU)
- National Association of Regulatory Utility Commissioners (NARUC)
- National Institute of Standards and Technology (NIST)
- National Public Safety Telecommunications Council (NPSTC)
- National Telecommunications and Information Administration (NTIA)
- New York City Department of Information Technology and Telecommunications (DoITT)
- North American Electric Reliability Council (NERC)
- Organization for the Promotion and Advancement of Small Telecommunications Companies (OPATSCO)
- President's National Security Technical Advisory Council (NSTAC)
- Securities Industry Association (SIA)

[7] These principles are carried forward from NRIC V and VI.

- United States Department of Homeland Security
  National Communications System (NCS)
  National Coordinating Center for Telecommunications (NCC)
  Telecom ISAC (Information Sharing and Analysis Center)
- United States Telecommunications Association (USTA)

2.3.7 Other Focus Groups

Because of the common areas of subject matter, the Wireless Network Reliability Focus Group needed to coordinate some activities. Liaisons were established between this Focus Group and each of the other NRIC VII Focus Groups.

Special coordination was required with the following Focus Groups in order to resolve Best Practice conflicting recommendations submitted by each Focus Group (FG). These Focus Groups were: FG 2A "Homeland Security-Infrastructure," FG 2B "Homeland Security-Cyber Security," FG 3B "Public Data Networks," and FG4 "Broadband."

2.3.8 Non-Disclosure Agreement

A Non-Disclosure Agreement was prepared by the NRIC VII Steering Committee to provide additional protection for parties that may bring sensitive information to the Focus Group for discussion.

2.3.9 Additional Wireless Workshops

2.3.9.1 Power Workshop- November 22, 2004

The goal of the Emergency Power Conference was to identify and address the unique challenges of providing emergency power to remote sites. It was held at the Bell Labs Network Reliability and Security Office (NRSO) in Washington, DC on November 22, 2004. Hosted by the IEEE, this workshop brought together 46 experts from the communications and electrical industries as well as representatives from government and academia. The learning's from this workshop (http://www.comsoc.org/~cqr/PowerConf.html) were studied by the Power Task Group and incorporated into the Focus Group's power recommendations.

2.3.9.2 RF Air Interface Workshop- May 17-18, 2005

The goal of our workshop was to get a group of industry RF air interface Subject Matter Experts (SMEs) together to generate Best Practices related specifically to the air interface. The 'RF Air Interface Workshop" for Wireless Network Reliability Focus Group 3A was held at the Bell Labs Network Reliability and Security Office (NRSO) in Washington, DC on May 17-18, 2005. There were 21 wireless industry experts in attendance of which 12 were RF Air Interface SMEs. The learnings from this workshop were studied by the Network Task Group and the RF SMEs and then incorporated into the Network Task Group's recommended Best Practices (Section 3.2.4.5).

2.3.9.3 Public Service Workshop – June 13-15, 2005

The goal of the Public Service Workshop was to generate discussion on the concerns of public entities regarding wireless networks. The workshop, hosted by the City of New York's Department of Information Technology and Telecommunications (DoITT), was attended by 26 experts from the wireless industry, city government, and various other industries. Highlights of the workshop included remarks from DoITT Commissioner Gino Menchini on the city's strategies for supporting a competitive wireless environment by advocating reasonable building top regulations for cell sites, establishing a competitive 'pole top' initiative and enhancing network reliability through redundant fiber and backup wireless initiatives.

In this dialogue, Mr. Menchini agreed that NRIC Best Practices are developed by experts and that not all Best Practices are applicable in all situations, Mr. Menchini supported the position of the implementation of Best Practices being voluntary.

Additional commentary from Peter Heuzey and Bruce Zenel of the Securities Industry Association (SIA) brought to light the increasing reliance upon wireless data services such as SMS and mobile email during disaster response activities.

The Wireless Networks Focus Group was able to utilize the insights gained in their work to refine the body of Best Practices to meet the needs of the wireless industry.

3 Analysis and Findings

3.1 Gap Analysis

The 12 gaps identified by this Focus Group are distributed across the communications infrastructure areas as follows:

Table 3.1. Distribution of Identified Gaps.

Area	Number of Gaps	Section
Environment	2	3.2.1
Hardware	0	3.2.2
Human	2	3.2.3
Network	3	3.2.4
Payload	1	3.2.5
Policy	1	3.2.6
Power	2	3.2.7
Software	1	3.2.8

3.2 Task Group Analysis

A Task Group was formed for each of the eight communications infrastructure areas. The number of new, modified or deleted Best Practices identified by each Task Group is identified in the following table.

Table 3.2.A. Focus Group 3A Task Group Best Practice Summary.

	ENVIRONMENT	**HARDWARE**	**HUMAN**	**NETWORK**	**PAYLOAD**	**POLICY**	**POWER**	**SOFTWARE**	**TOTAL**
New Best Practices	**4**	**1**	**1**	**32**	**1**	**4**	**8**	**0**	**51**
Modified Best Practices	**6**	**0**	**0**	**4**	**2**	**1**	**1**	**8**	**22**
Deleted Best Practices	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

The following table provides the total number of new, modified or deleted Best Practices that were identified by each of the three processes used by each of the eight Task Groups. These processes are:

- Wireless Network Gap Closure Process
- Wireless Network Effectiveness Survey Process
- Wireless Network Services Applicability Improvement Process

Table 3.2.B. Focus Group 3A Best Practice Summary.

	Gap Closure Process (12 Gaps)	Effectiveness Survey Process	Services Applicability Improvement Process	TOTAL
New Best Practices	43	0	8	**51**
Modified Best Practices	5	8	9	**22**
Deleted Best Practices	0	0	0	**0**

3.2.1 ENVIRONMENT

3.2.1.1 Environment Subject Matter

Environmental considerations play a critical role in the reliability of wireless networks. The Environment category includes the broad array of conditions that may impact the sustained reliability of general, and wireless specific, network infrastructure. This infrastructure includes buildings and equipment, tower sites and landscaping that are part of communications systems. Environmental factors may influence architecture, engineering, maintenance routines, restoration efforts, hazardous material handling, and business continuity programs.

Virtually everything related to the communications infrastructure happens in an "environment" such as a building, an Internet portal, a communications tower, etc. Each of these "environments" is also influenced and affected by "environmental" factors such as fire, floods, ice and snow. Some factors relating to the environment can be controlled or mitigated [through the use of Best Practices] and some cannot, making the task of protecting communications infrastructure an incredible challenge.[8] In addition to the "natural" environmental conditions' potential to adversely impact network reliability, this scope area also encompasses the potential for both intentional and unintentional manmade environmental impacts.

3.2.1.2 Environment Task Group Participants

The Environment Task Group assembled a team of sufficient expertise to effectively address environmental subject matter as it relates to the reliability of networks in general, and wireless networks in particular. The Environment Task Group was made up of 10 participants. The Task Group was further segmented into the following areas of expertise:

- ❑ Business Continuity
- ❑ Hazardous Material
- ❑ Buildings
- ❑ Equipment
- ❑ Tower Sites
- ❑ Landscape

A knowledgeable Task Group member was solicited to facilitate each section of expertise. In addition to members of the Focus Group, the Task Group engaged other subject matter experts to strengthen its expertise as needed. Table 3.2.1.2 lists the Environment Task Group participants. Care was also taken to include representation from a broad range of industry roles as well as from different technologies. The team had sufficient expertise to complete this activity.

[8] Network Reliability and Interoperability Council VII, Focus Group 3A, Initial Report

Table 3.2.1.2. Environment Task Group Participants.

Name	Organization
Victor DeVito, ***Leader***	AT&T
Julie Briggs	AT&T
Ralph Collipi	AT&T
Linda Ferro	AT&T
Eric Hounchell	Battery Corp
Miles Schreiner	T-Mobile
John Chapa	SBC
Jim Runyon	Bell Labs, Lucent Technologies
Ted Abrams	American Tower Corporation

3.2.1.3 Environment Summary

The Environment Task Group methodology was to develop Best Practices by identifying and closing gaps as they pertain to wireless networks/infrastructure, and through evaluation/recommendations from the results of the Effectiveness Survey. The following table summarizes the results of the Best Practices resulting from each of these activities. Subsequent sub-sections will provide additional details for each of the activities defined in the methodology.

Table 3.2.1.3. Environment Task Group Summary of Best Practice Activities.

	Gap Closure Process (2 Gaps)	Effectiveness Survey Process	Wireless Services Applicability Improvement Process	TOTAL
New Best Practices	3	0	1	**4**
Modified Best Practices	2	4	0	**6**
Deleted Best Practices	0	0	0	**0**

3.2.1.4 Environment Gap Analysis

The Council Charter directs the Focus Group to "*perform a gap analysis to determine areas where new Best Practices for Wireless Network providers are needed*." As described in Section 2.3.5, the approach used for the Environment Team was similar for the other areas. Therefore, a gap is here defined as a space between the known problems associated with environment factors that can impact network reliability, and the existing body of Best Practices that address these factors. To understand the former boundary, the entire FG 3A Team generated a brainstormed list of 55 known issues, and potential Best Practice Environment items. These issues and potential Best Practice items were grouped into the previously identified areas of expertise, and were consolidated to eliminate duplication.

To understand the latter boundary, the entire body of existing Best Practices from the previous NRIC's was reviewed and researched. Forty Best Practices identified through the areas of expertise were found to have application to the reliability of wireless networks[9] and satisfactorily addressed to varying degrees a particular environmental issue or item initially identified by the FG 3A Focus Group.

The Task Group's gap analysis determined that while the majority of the identified issues and items generated by FG 3A had existing Best Practices to mitigate the threat posed by that particular issue or item, there were gaps to the issues/items list found in some of the areas of expertise. In particular, while the Hazardous Material and Weather sub-category issues/items were completely covered through consolidation and existing Best Practice documentation, the remaining areas were not adequately addressed solely by existing Best Practices and required further review.

The task group has identified the following two Gaps:

Business Continuity Planning
Existing Best Practices do not address potential impacts of collateral damage from adjacencies.

Cell Site Administration:
Areas of concern include adhering to engineering designs, signage considerations, rogue equipment identification, and bird populations.

3.2.1.5 Environment Gap Closure

From the Environment Team's analysis of all issues/items initially brainstormed by the Focus Group which were not fully mitigated or documented through existing practices, five new or edited Best Practices were researched, proposed, and recommended back to the FG 3A Team for overall Focus Group approval.[10] Final statistics indicate that three new practices and two revisions to existing Best Practices have been reviewed and approved by the Focus Group. The following three new NRIC Best Practices have been identified to specifically address the gaps that were identified by the Environment Task Group.

- **7-P-0450** Property Managers should maintain current documentation that ensures that the tower loading is consistent with the engineering design (e.g., antenna loading, feedline loading, ice or wind loading).

[9] An NRIC Best Practices web site search for the various areas of expertise under study revealed the following forty Best Practices as applicable to the environmental issues and items: 6-6-5072, 6-6-5073, 6-6-1004, 6-5-0599, 6-6-5207, 6-6-1067, 6-5-0655, 6-5-0699, 6-6-5204,6-6-5214, 6-6-5232, 6-6-5275, 6-5-0597, 6-5-0588, 6-6-1001, 6-6-0577, 6-6-8068, 6-6-5259, 6-6-1020, 6-6-1051, 6-6-5138, 6-6-5139, 6-6-5064, 6-6-5119, 6-6-5006, 6-6-5008, 6-6-5021, 6-6-5011, 6-6-5012, 6-6-5026, 6-5-0723, 6-5-0651, 6-5-0652, 6-6-5120, 6-6-5149, 6-6-5229, 6-6-5239, 6-5-0658, 6-6-5197, 6-6-5145

[10] The Task Group also recognized that there were a number of issues/items (5 total) that were more appropriate to be addressed by the Hardware (1 item), Power (1 item), and Policy (3 items). With agreement from the Task Team leaders, these items were assigned to the new task team for review and recommendation. In addition, the Task Group recognized 1 item as generalized Areas for Attention for physical Homeland Security Focus Group 2A, but does not see them as specific to Wireless Network Environment issues. These items were recommended and accepted for transfer to that NRIC Focus Group.

- **7-P-0451** Service Providers, Network Operators and Property Managers should conduct a periodic physical site audit to update and maintain accurate antenna and tower engineering documentation in order to positively identify every item on the tower structure (e.g., identifying rogue antennas).

- **7-P-0452** Service Providers, Network Operators and Property Managers should post emergency contact number(s) and unique site identification in an externally visible location at unmanned communication facilities (e.g., towers, cell sites, Controlled Environment Vault (CEV), satellite earth stations). This signage should not reveal additional information about the facility, except when necessary.

Verbiage modification to two existing Best Practices also contributed to address the gap issues.

- **7-P-5072** Service Providers, Network Operators and Equipment Suppliers should perform risk assessments on key network facilities and control areas on a regular basis. Assessments should address natural disasters and unintentional or intentional acts of people on facility or nearby structures.

- **7-P-5145** Network Operators should establish plans to perform interference analysis and mitigation to ensure timely resolution of all cases of interference (e.g., caused by equipment failure, intentional act/sabotage or frequency overlap). Where feasible, analysis should enable identification of type and general location of interference source.

Specific concerns and additional Best Practices unique to avian issues were identified and recommended for approval based on analysis performed as part of the Air Interface Workshop (Facilities) sub-team efforts. This successfully closed each of the Environment gap issues identified through the process.

3.2.1.6 Environment Effectiveness Survey Process

The Environmental Best Practices selected for the Effectiveness Survey were for the most part rated effective or moderately effective. However, there were three Best Practices evaluated as less effective. Respondent comments indicated that while the Practices themselves were effective, the verbiage defining the practice was not. Additionally, a fourth Best Practice with a highly effective rating had one respondent rate the practice as ineffective due to verbiage issues. As a result, the Environment sub-team has recommended to the Focus Group the revised wording for four additional Best Practices as a result of the Effectiveness Survey.

- **7-P-1020** Service Providers, Network Operators, and Equipment Suppliers should assess the need for Chemical, Biological, Radiological and Nuclear (CBRN) response program to safely restore or maintain service in the aftermath of fuel/chemical contamination or a Weapons of Mass Destruction (WMD) attack.

- **7-P-5064** Service Providers, Network Operators and Property Managers should alarm and monitor critical electronic equipment areas to detect parameters that are outside operating specifications (e.g., temperature, humidity).

- **7-P-5089** Service Providers, Network Operators and Equipment Suppliers should establish, implement and enforce appropriate procedures for the storage and movement of equipment and material, including trash, around facilities and campuses.

- **7-P-5139** Service Providers, Network Operators and Equipment Suppliers should consider establishing procedures for managing personnel who perform functions at disaster area sites.

3.2.1.7 Environment Services Applicability Improvement Process

Per the NRIC VII charter, the Wireless Network Focus Group was to "refine existing Best Practices to improve their applicability to wireless networks."

The Task Group was assigned issues of concern, some of which were identified as gaps in existing Best Practices (see Section 3.2.1.4). Other issues required actions to be taken to create new or modify existing Best Practices. For the Environment Task Group, in addition to the gap closure items, an additional Best Practice was proposed, reviewed and accepted by the Focus Group for final approval by the Council.

- **7-P-0453** Service Providers and Network Operators should prepare for HVAC or cabinet fan failures by ensuring that conventional fans are available to cool heat-sensitive equipment, as appropriate.

3.2.1.8 Environment Issues for Further Investigation

Based on scope and known processes in place, there were no outstanding issue requiring further investigation and assessment.

3.2.2 HARDWARE

3.2.2.1 Hardware Subject Matter

Hardware has a fundamental and critical role in the reliability of wireless networks. The Hardware area includes the broad category of physical electronics and related components that are part of communications systems. Hardware systems include both passive and active devices. Passive devices include such items as antennas, buildings, cabinets, cabling, frames, racks, and structures that provide the necessary physical, environmental, and communication support for active electronic elements. Active electronic devices used in wireless systems include such items as radio receivers and transmitters, controllers, concentrators, aggregators, servers, routers, and switches. Wireless Systems are experiencing a convergence of traditional wireless voice telephony architectures with Internet Protocol based computer networks enabling the system operators to offer a feature-rich suite of applications (e.g. voice, text, video) to their customers. The resulting network designs incorporate hardware from many different equipment suppliers located in facilities as small as a broom closet containing a concentrator, to multi-story buildings containing many concentrators, switches and routers from many different equipment suppliers.[11]

3.2.2.2 Hardware Task Group Participants

The Hardware Task Group assembled a team of cross manufacturer expertise to effectively address the Hardware subject matter as it relates to the reliability of wireless networks. The Hardware Task Group was made up of participants from U.S. wireless and data equipment manufacturers. Additionally, members of the full Focus Group were engaged in the discussion and review of proposed revisions and additions to the Best Practices. Table 3.2.2.2 lists the Hardware Task Group participants. Care was also taken to include representation from a broad range of industry roles as well as from different technologies. The team had sufficient expertise to complete this activity.

Table 3.2.2.2. Hardware Task Group Participants.

Name	Organization
Robin Roberts	Cisco Systems
Rick Krock	Bell Labs, Lucent Technologies
Lester Buczek, ***Co-Leader***	Motorola
John Bassett, ***Co-Leader***	Motorola
Bentley Alexander	Ericsson

3.2.2.3 Hardware Summary

The Hardware Task Group methodology was to develop Best Practices by identifying and closing gaps, identifying Wireless service applicability and implementing the results of the Effectiveness Survey. The following table summarizes the results of the Best Practices resulting from these activities. Subsequent sub-sections will provide additional details for each of the activities defined in the methodology.

[11] Network Reliability and Interoperability Council (NRIC) VI Homeland Security Physical Security Focus Group Final Report, Issue 3, December 2003, p. 49. (www.nric.org)

Table 3.2.2.3. Hardware Task Group Summary of Best Practice Activities.

	Gap Closure Process (1 Gap)	Effectiveness Survey Process	Wireless Services Applicability Improvement Process	TOTAL
New Best Practices	0	0	1	**1**
Modified Best Practices	0	0	0	**0**
Deleted Best Practices	0	0	0	**0**

3.2.2.4 Hardware Gap Analysis

The Council Charter directs the Focus Group to "*perform a gap analysis to determine areas where new Best Practices for [Wireless Network] providers are needed*." The approach used for Hardware was similar to the process used in other areas as described in Section 2.3.5. Therefore, a gap is here defined as a space between the known problems associated with Hardware that can impact network reliability and the existing Best Practices for Hardware. To understand the former boundary, a list was generated of 21 known concerns for Hardware. To understand the latter boundary, the existing Best Practices were researched and 54 were found to have potential application to the reliability of wireless networks.[12] In addition, the Task Group reviewed the work of the previous Council in which the vulnerabilities of Hardware were systematically reviewed.[13]

The task group identified no Gaps.

3.2.2.5 Hardware Gap Closure

The Task Group's gap analysis determined that there were no significant gaps in the Hardware area, several new practices were identified for consideration and discussion in the full Focus Group forum. The full Focus Group agreed two of these proposed practices should be included in Best Practices documentation. The Task Group found all of the 54 existing Best Practices to be relevant for wireless networks.

3.2.2.6 Hardware Effectiveness Survey Process

The ten individual Hardware Best Practices selected for the Effectiveness Survey were rated as effective or moderately effective. Collectively, 96% of the valid responses rated the survey BPs as either effective or moderately effective. As such, no modifications were required.

[12] An NRIC Best Practices web site keyword search for "hardware" returns the following 54 Best Practices: 6-5-0501, 6-5-0504, 6-5-0510, 6-5-0541, 6-5-0548, 6-5-0553, 6-5-0554, 6-5-0557, 6-5-0559, 6-5-0590, 6-5-0600, 6-5-0614, 6-5-0618, 6-5-0620, 6-5-0622, 6-5-0657, 6-5-0664, 6-5-0699, 6-5-0702, 6-5-0745, 6-5-0749, 6-5-0750, 6-6-1066, 6-6-5030, 6-6-5061, 6-6-5064, 6-6-5080, 6-6-5081, 6-6-5082, 6-6-5083, 6-6-5084, 6-6-5085, 6-6-5086, 6-6-5088, 6-6-5098, 6-6-5117, 6-66-5118, 6-6-5119, 6-6-5148, 6-6-5149, 6-6-5171, 6-6-5194, 6-6-5195, 6-6-5198, 6-6-5200, 6-6-5202, 6-6-5219, 6-6-5230, 6-6-5237, 6-6-5245, 6-6-5262, 6-6-5277, 6-6-5278, 6-6-5279.

[13] *A characteristic of any aspect of the communications infrastructure that renders it, or some portion of it, susceptible to damage or compromise.* NRIC VI Homeland Security Physical Security Focus Group Final Report, Issue 3, December 2003, p. 39.

The Task Group received specific comments from the survey respondents on three of the Best Practices:

- 6-6-5202
- 6-6-1046
- 6-6-1066

The comments for these three BPs, as well as the survey responses from all ten BP's were reviewed during a meeting of the full Focus Group. The Focus Group referred one of the three BPs, 5202, back to the Hardware Task Group for further discussion and modification. Separately, Focus Group 2A (Infrastructure) also reviewed 5202 and recommended deletion. FG2A proposed a modification to another existing BP, 5263, as a replacement for 5202.

The 3A Hardware Task Group determined the 2A proposed modifications to BP 5263 addressed its concerns. The Task Group concurred with FG2A recommendations to delete 5202.

3.2.2.7 Hardware Services Applicability Improvement Process

Per the NRIC VII charter, the Wireless Focus Group was to "refine existing Best Practices to improve their applicability to the wireless industry."

The Task Group approached this task by reviewing existing Best Practices pertaining to hardware, concerns raised during the Gap Analysis, and feedback received from respondents to the full Group's BP Effectiveness Survey. The Hardware Task Group crafted and recommended one new Best Practice.

- **7-P-0455** Equipment Suppliers should consider a program to remove cards or modules from circulation that have a history of failure even if tests indicate "No Trouble Found".

3.2.2.8 Hardware Issues for Further Investigation

Based on the scope and known processes in place, there were no issues identified by the Hardware Task Group that will require further investigation.

3.2.3 HUMAN

3.2.3.1 Human Subject Matter

The Human vulnerabilities were analyzed with consideration to external threat to the wireless networks (in the form of attacking one or more network elements) as well as threats to the personnel (such as hijacking, kidnapping or blackmailing). Additionally, both intentional threats from external (e.g., terrorism, vandalism) and from the communications personnel to the network (e.g., from disgruntled employees) as well as unintentional threats from communications personnel to the network (e.g., human errors caused due to confusion, anxiety, etc.) were considered.

3.2.3.2 Human Task Group Participants

The Task Group leaders ensured that sufficient expertise was engaged to address the Human vulnerabilities. The Human Task Group was made up of five participants. The table below lists the Human Task Group participants. Care was taken to include representation from different industry segments such as Service Providers, Network Operators and Equipment Suppliers. The team took the approach of engaging many members of the Focus Group 3A to review concerns about existing Best Practices from previous NRIC Focus Groups. Table 3.2.3.2 lists the Human Task Group participants.

Table 3.2.3.2. Human Task Group Participants.

Name	Organization
John Quigley, ***Leader***	Sprint
William Hitchcock	Sprint
David Proffer	Nextel
Anil Macwan	Bell Labs, Lucent Technologies
Rick Krock	Bell Labs, Lucent Technologies

3.2.3.3 Human Summary

The Human Task Group methodology was to develop Best Practices by identifying and closing gaps, identifying wireless service applicability, and implementing the results of the Effectiveness Survey. The following table summarizes the results of the Best Practices resulting from these activities. Subsequent sub-sections will provide additional details for each of the activities defined in the methodology.

Table 3.2.3.3. Human Task Group Summary of Best Practice Activities.

	Gap Closure Process (2 Gaps)	Effectiveness Survey Process	Wireless Services Applicability Improvement Process	TOTAL
New Best Practices	1	0	0	**1**
Modified Best Practices	0	0	0	**0**
Deleted Best Practices	0	0	0	**0**

3.2.3.4 Human Gap Analysis

The Council Charter directs the Focus Group to "provide a report describing the results of the gap analysis of Best Practices aimed at the reliability of wireless networks". The approach used for Human was similar to the process used in other areas as described in Section 2.3.5. Therefore, a gap is here defined as a space between the known problems associated with human vulnerabilities that can impact network reliability and the existing Best Practices that address human issues. To understand the former boundary, a list was generated of 22 known concerns for the Human area. To understand the latter boundary, the existing Best Practices pertaining to human issues (approximately 100)[14] were researched and most of the identified concerns were found to be adequately addressed by existing Best Practices. In addition, many of the existing human Best Practices apply to various aspects of wireless networks.

The remaining issues that are not adequately addressed by existing Best Practices are defined as gaps.

The task group has identified the following two Gaps:

Technical Support and Escalation

Ensure timely engagement of technical support at the appropriate level during an outage.

Offshore Network Operations Control Centers (NOCC)

Location of NOCCs outside of the US poses some potential risk to the management and security of telecommunication networks.

3.2.3.5 Human Gap Closure

NRIC VI identified three Best Practices[15] that are applicable to technical support. However, in order to fully address the first gap, the following new NRIC Best Practice has been defined.

- **7-P-0454** Network Operators and Service Providers should consider establishing technical and managerial escalation policies and procedures based on the service impact, restoration progress and duration of the issue.

With respect to the second gap, NRIC VI identified three Best Practices[16] related to securing sites in foreign countries. Through research, the Human Task Group was

[14] An NRIC Best Practices web site keyword search for "human resources", "training and awareness" and "supervision" returns the following 112 Best Practices: 6-5-0502, 6-5-0504, 6-5-0510, 6-5-0511, 6-5-0516, 6-5-0533, 6-5-0535, 6-5-0537, 6-5-0541, 6-5-0542, 6-5-0548, 6-5-0549, 6-5-0551, 6-5-0557, 6-5-0560, 6-5-0564, 6-5-0565, 6-5-0574, 6-5-0578, 6-5-0579, 6-5-0588, 6-5-0589, 6-5-0590, 6-5-0592, 6-5-0593, 6-5-0595, 6-5-0597, 6-5-0598, 6-6-0599, 6-5-0600, 6-5-0604, 6-5-0609, 6-5-0617, 6-5-0629, 6-5-0631, 6-5-0650, 6-5-0671, 6-5-0697, 6-5-0711, 6-5-0713, 6-5-0729, 6-5-0751, 6-5-0756, 6-6-0760, 6-6-5001, 6-6-5008, 6-6-5015, 6-6-5016, 6-6-5018, 6-6-5019, 6-6-5021, 6-6-5023, 6-6-5027, 6-6-5028, 6-6-5031, 6-6-5032, 6-6-5033, 6-6-5034, 6-6-5037, 6-6-5050, 6-6-5054, 6-6-5055, 6-6-5062, 6-6-5065, 6-6-5067, 6-6-5068, 6-6-5070, 6-6-5091, 6-6-5093, 6-6-5094, 6-6-5095, 6-6-5096, 6-6-5114, 6-6-5115, 6-6-5116, 6-6-5125, 6-6-5126, 6-6-5127, 6-6-5128, 6-6-5134, 6-6-5138, 6-6-5139, 6-6-5140, 6-6-5155, 6-6-5160, 6-6-5164, 6-6-5165, 6-6-5168, 6-6-5175, 6-6-5178, 6-6-5179, 6-6-5184, 6-6-5192, 6-6-5193, 6-6-5196, 6-6-5203, 6-6-5208, 6-6-5217, 6-6-5221, 6-6-5244, 6-6-5256, 6-6-5257, 6-6-5258, 6-6-5260, 6-6-5265, 6-6-5266, 6-6-5267, 6-6-5269, 6-6-5270, 6-6-5275, 6-6-5277, 6-6-5278

[15] Obtained via the NRIC VI Best Practice web site using text search with 'Technical Support.'

unable to find any existing practices with domestic carriers operating their network control centers on foreign soil. It is therefore the recommendation of the Focus Group that any entity contemplating locating such a center internationally adhere to the following existing NRIC Best Practices:

- **6-6-5220** – Service Providers, Network Operators and Equipment Suppliers who utilize foreign sites should establish and implement a comprehensive physical security program for protecting corporate assets at those sites.

- **6-6-5279** – Service Providers, Network Operators and Equipment Suppliers should be aware that some environments around the world present higher and/or different risks than others, and regional-specific threat information should be taken into consideration during security program development.

3.2.3.6 Human Effectiveness Survey Process

The Human Best Practices selected for the Effectiveness Survey were rated as 97% effective or moderately effective and, as such, no modifications were required. Of the remaining 3%, the Task Group reviewed the comments from the survey and drafted proposed modifications to resolve those issues. The proposed modifications were submitted to Focus Group 2A as the specific Best Practices in question fell under their purview.

3.2.3.7 Human Services Applicability Improvement Process

Per the NRIC VII charter, the Wireless Best Practices Focus Group was to “refine existing Best Practices to focus their applicability to the wireless industry.”

The Task Group was assigned issues of concern, some of which were identified as gaps in existing Best Practices (see Section 3.2.3.4). Other issues required actions to be taken to create new or modify existing Best Practices. For the Human Task Group, all the identified issues were addressed by existing Best Practices.

3.2.3.8 Human Issues for Further Investigation

Based on scope and known processes in place, there are some issues that will require further investigation. For the Human area, there were no items identified for further investigation.

[16] Obtained via the NRIC VI Best Practice web site using text searches with ‘Foreign Security’ and ‘Security.’

3.2.4 NETWORK

3.2.4.1 Network Subject Matter

The Network Task Group for Focus Group 3A has taken into consideration all of the network switching, radio, and transport elements required to inter-connect a wireless network. Previous Councils have looked at Reliability, Business Continuity, Network Design, Network Elements, Network Operations, Policy, Procedures, and Network Provisioning from a wireline perspective. The Wireless Network Task Group will take into consideration the wireline aspects of a wireless network but will focus on the Radio Access Network that allows a mobile phone to connect to the wired network. The Task Group focused on improving the reliability of wireless networks by addressing Design/Planning, Operational, Administrative, Maintenance and Provisioning Best Practices that are relevant to wireless networks.

Design and Planning: The activities associated with continuing to provide for the increasing demands on wireless networks. Examples include design for new facilities, cell sites, capacity augments, and business continuity planning.

Operations: The day-to-day activities associated with keeping the wireless networks operating reliably and efficiently. Examples include network monitoring, maintenance, fault management, drive testing, reviewing key performance indicators.

Administration: Includes all activities associated with managing the network assets, co-ordination of field personnel, reporting on the network status, and data basing key network information on circuit IDs, switch and cell site locations, etc.

Maintenance: The ongoing corrective or preventive activities associated with keeping the network operating. Includes planned and unplanned maintenance activities. Planned maintenance is preventive action to prevent network disruptions. Unplanned maintenance is in response to a sudden unexpected network disruption.

Provisioning: Supplying telecommunications services to a wireless user, including all associated transmission, wiring, and equipment. Examples include providing the sufficient quantities of network elements and circuits and configuring them to meet service level standards.

3.2.4.2 Network Task Group Participants

The Network Task Group assembled a diverse team of 6 individuals with representatives that include equipment suppliers and network/service providers. In addition to members of the Task Group, subject matter experts were engaged to strengthen its expertise and develop Best Practices. Table 4.2.4.2 lists the Network Task Group participants.

Table 3.2.4.2. Network Task Group Participants.

Name	Organization
Brad McManus, ***Leader***	Sprint
Steven J. Paton	ALLTEL
Mark Adams	Cox Communications
Jim Runyon	Bell Labs, Lucent Technologies
Srini Anam	Nortel Networks

Sherman Philips	Qwest Wireless

3.2.4.3 Network Summary

The Network Task Group methodology was to develop Best Practices by identifying and closing gaps, identifying Wireless service applicability and implementing the results of the Effectiveness Survey. The following table summarizes the results of the Best Practices resulting from these activities. Subsequent sub-sections will provide additional details for each of the activities defined in the methodology.

Table 3.2.4.3. Network Task Group Summary of Best Practice Activities.

	Gap Closure Process (3 Gaps)	Effectiveness Survey Process	Wireless Services Applicability Improvement Process	TOTAL
New Best Practices	29	0	3	**32**
Modified Best Practices	1	0	3	**5**
Deleted Best Practices	0	0	0	**0**

3.2.4.4 Network Gap Analysis

The Council Charter directs the Focus Group to "*perform a gap analysis to determine areas where new Best Practices for wireless networks are needed*." The approach used for Network was similar to the process used in other areas as described in Section 2.3.5.

As a starting point and to encourage free form and innovative thinking the Focus Group 3A and Network Task Group used brainstorming methods or submittals by industry experts to detail a listing of 115 potential concerns for the network area of wireless networks. The 115 concerns were subsequently investigated and discussed by the Network Task Group to determine if they were applicable to wireless networks or were a good candidate for a potential Best Practice.

By analysis, the 115 concerns were consolidated into a more concise list of potential Best Practices candidates applicable to wireless networks. The list underwent detailed analysis to determine the proper disposition. The following dispositions were use to address the gaps within the Task Group:

- new Best Practices
- addressed by an existing Best Practice
- modified an existing Best Practice
- transferred to another Task Group
- consolidate with other potential issues on the list
- out of scope or not applicable to wireless networks

The task group identified the following three gaps:

Business Continuity Related to Wireless Networks

There are a number of Best Practices addressing business continuity for communication networks. However, existing NRIC Best Practices do not provide guidance for cell site prioritization and contingency planning for key coverage areas.

Air Interface Reliability
The Network Task group has identified insufficient guidance in existing Best Practices for the unique challenges related to the planning, engineering and optimization of the air interface.

Cell Site Administration
The Network Task group identified the need to gather and maintain cell site information related to the performance, connectivity, and maintenance.

3.2.4.5 Network Gap Closure

From the Network Team's analysis of all issues/items initially brainstormed by the Focus Group and the RF air interface workshop in May which were not fully mitigated or documented through existing practices, 37 new and 10 edited Best Practices were researched, proposed, and recommended back to the FG 3A Team for overall Focus Group approval. The following Best Practices have been written to specifically address the gaps that were identified by the Network Task Group.

Business Continuity Related to Wireless Networks
The following two new Best Practices address the Business continuity gap.

- **7-P-0459** Equipment Suppliers should design outdoor equipment (e.g., base station) to operate in expected environmental conditions (e.g., weather, earthquakes).

- **7-P-0461** Equipment Suppliers should provide the capability to test failover routines of redundant network elements.

Verbiage modification to one existing Best Practices also contributed to address the Business continuity gap issues.

- **7-P-1026** Service Providers and Network Operators should consider creating a corporate policy statement that defines a remote system access strategy, which may include a special process for disaster recovery.

Air Interface Reliability
The following 15 new Best Practices address the Air Interface Reliability gap.

- **7-P-0457** Network Operator and Service Provider should develop a process to identify RF dead spots and, where feasible, provide a solution to fill the dead spot with RF coverage.

- **7-P-0458** Network Operator should verify when a new cell site is added to the network that calls handoff between cells.

- **7-P-0464** Network Operators and local municipalities should cooperate on zoning issues that affect reliability of communication networks serving the public good (e.g., noise from emergency backup power generators, aesthetics of tower placement, public safety and health concerns).

- **7-P-0465** Network Operators should, during the initial design and periodic reviews of cell site coverage, account for the effects of environmental changes (e.g., new buildings, tree growth, construction materials) that result in attenuation, shadowing, and multipath.

- **7-P-0466** Network Operators should, when planning network coverage, take into account link budget impacts due to propagation differences between various spectrum (e.g., 850 MHz vs. 1800/1900 MHz).

- **7-P-0467** Network Operators should give consideration to the degree of balance between RF channels on uplinks and downlinks, for both control and traffic.

- **7-P-0477** Network Operators, when designing cell sites with high voltage FAA beacons, should consider the potential of electromagnetic coupling into the receivers and, if present, take appropriate steps to mitigate the interference (e.g., squelch, physical separation, shielding).

- **7-P-0479** Network Operators should take into consideration fundamental technology differences when operating multiple RF technologies in an existing system. Radio Frequency Interference (RFI) sources (e.g., intermodulation, out of band emissions, receiver overload), link budgets, and performance metrics (e.g., data rates, latency, capacity) should be evaluated.

- **7-P-0480** Network Operators and Property Managers should periodically inspect antennas, waveguide, and ancillary hardware to insure physical integrity and the absence of physical movement which can create intermittent and localized intermodulation interference generators (e.g., rusty joints) and/or alter predicted antenna radiation patterns (e.g., antennas swinging around in the wind) potentially creating interference.

- **7-P-0482** Network Operators should utilize RF propagation and other modeling tools to analyze and optimize designs to avoid interference and improve network performance.

- **7-P-0483** Network Operators should have a master cell site database with configuration parameters, connectivity, and performance statistics that can be used to analyze and audit cell site performance.

- **7-P-0484** Network Operators should have a program (e.g., automated drive test equipment, network probes) to monitor and detect network performance anomalies.

- **7-P-0485** Network Operators should optimize cell sites, including relationships between neighboring cells, using a combination of drive testing and network statistics.

- **7-P-0486** Network Operators should have an ongoing RF performance improvement process to reduce blocks, drops, and access failures.

- **7-P-0487** Network Operators should have procedures in place to identify and correct degradations in cell site performance resulting from defects in feedlines and antennas (e.g., moisture, bullets, kinking).

Cell Site Administration
The following 12 new Best Practices address the Cell Site Administration gap.

- **7-P-0456** Network Operators should maintain records of pertinent information related to a cell site for its prioritization in disaster recovery and key coverage areas (e.g., emergency services, government agencies, proximity to hospitals).

- **7-P-0468** Network Operators and Property Managers should consider agreements to share in-building antenna infrastructure between multiple service providers in order to make it more feasible to deploy in-building systems.

- **7-P-0469** Network Operators and Property Managers should consider the use of cable support (e.g., H-Frames, Ice Bridges) in tower and shelter designs.

- **7-P-0470** Network Operators and Property Managers should consider tower and antenna designs that do not attract bird and animal nesting (e.g., no platforms, flush mounted panels, smooth radome).

- **7-P-0471** Network Operators and Property Managers should consider remote, electronic antenna aiming and utilize tower-mounted equipment that minimizes the need for tower top maintenance where conditions prevent climbs (e.g., osprey nest, weather conditions).

- **7-P-0472** Network Operators and Equipment Suppliers should consider connector choices and color coding to prevent inappropriate combinations of RF cables.

- **7-P-0473** Property Managers should consider maintaining a list of authorized climbers and a log of authorized tower climbs.

- **7-P-0474** Network Operators and Property Managers should periodically perform grounds maintenance at cell site facilities (e.g., pest control, mow grass, fence maintenance, snow removal).

- **7-P-0475** Network Operators and Property Managers should have agreements in place to ensure necessary and timely access to cell sites.

- **7-P-0476** Network Operators and Property Managers should consider conducting physical site audits after a major event (e.g., weather, earthquake, auto wreck) to ensure the physical integrity and orientation of hardware has not been compromised.

- **7-P-0478** Network Operators, when designing cell sites, should allow for deviation in elevation angle and azimuth resulting from deflection of the supporting structure (e.g., sun, load distribution, wind).

- **7-P-0481** Network Operators and Property Managers should ensure appropriate spacing between all antennas at a cell site in order to avoid interference, intermodulation, or other detrimental effects.

3.2.4.6 Network Effectiveness Survey Process

The Network Best Practices selected for the Effectiveness Survey were rated as 98% effective or moderately effective and, as such, no modifications were required. Of the remaining 2%, the Task Group reviewed the comments from the survey and drafted proposed modifications to resolve those issues. The proposed modifications were submitted to Focus Group 2A as the specific Best Practices in question fell under their purview.

3.2.4.7 Network Service Applicability Improvement Process

Per the NRIC VII charter, the Wireless Best Practices Focus Group was to “refine existing Best Practices to focus their applicability to the wireless industry.”

The Task Group was assigned issues of concern, some of which were identified as gaps in existing Best Practices (see Section 3.2.4.4). Other issues required actions to be taken to create new or modify existing Best Practices. For the Network Task Group, three new issues were addressed.

- **7-P-0460** Network Operators should ensure that equipment is installed in accordance with equipment suppliers' stated environmental specifications.

- **7-P-0462** Network Operators should work in conjunction with local municipalities to anticipate RF capacity needs driven by changes in vehicle traffic patterns or other demographics.

- **7-P-0463** Network Operators and Service Providers should consider establishing agreements so that mobile customers can roam on other providers' networks.

Verbiage modification to three existing Best Practices also contributed to address the Business continuity gap issues.

- **7-P-0555** Equipment Suppliers should continually enhance their software development methodology to ensure effectiveness by employing modern processes of assessment.
- **7-P-0565** Equipment Suppliers should establish and use metrics to identify key areas and measure progress in improving quality, reliability, and security during product development and field life cycle.

- **7-P-0805** Service Providers, Network Operators and Equipment Suppliers should work to establish operational standards and practices that support broadband capabilities and interoperability (e.g., video, voice, data, landline, wireless).

3.2.4.8 Network Issues for Further Investigation

For the Network area, there were no items identified for further investigation.

3.2.5 PAYLOAD

3.2.5.1 Payload Subject Matter

The payload in wireless networks is increasingly becoming an essential element in the continued operation of our nation's communications infrastructure. The payload in these networks can be described as consisting of two types of data: the "signaling" information that is essential to call management (e.g., call set up); and, the end-user "bearer" information consisting of the information (e.g., voice, data) that the end-user transmits or receives.

Compromises to the payload could expose companies, cities, or even countries to severe and dangerous consequences. Attacks against payload could disrupt or otherwise compromise critical communications or operations during an emergency situation, or could in themselves precipitate an emergency situation.

In wireless networks, the unique payload concerns are related to the air interface between the end-user and the core network. Payload carried over this air interface must be protected from 1) interception, 2) modification, 3) interruption or 4) interference.

The payload area is multi-dimensional and should include consideration of: In-band signaling control, potential payload corruption, potential payload interception, bandwidth constraints associated with payload spikes and air link overload, payload blocking, payload corruption, payload encryption, payload encapsulation, the unpredictability of payload, and a dependency on the proper functioning of the RF carrier.

Wireless payload, whether voice or data, is the major source of communication as well as a major component of commerce, public safety, transportation, national security, and emergency response. Payload loss, whether directly or through the loss of the infrastructure, could have a devastating effect on an affected region or the entire nation.

3.2.5.2 Payload Task Group Participants

The Payload Task Group assembled a team of sufficient expertise to effectively address the payload subject matter as it relates to the reliability of wireless networks. The Payload Task Group was made up of 6 participants. In addition to members of the Focus Group, the Task Group engaged other subject matter experts to strengthen its expertise. Table 4.2.5.2 lists the Payload Task Group participants. The team had sufficient expertise to complete this activity.

Table 3.2.5.2. Payload Task Group Participants.

Name	Organization
Bentley Alexander	Ericsson
Sunil Bhojwani	Sprint
David Proffer	Nextel
Karl Rauscher	Bell Labs, Lucent Technologies
Jim Runyon, ***Leader***	Bell Labs, Lucent Technologies
Mike Sheffield	MCI

3.2.5.3 Payload Summary

The Payload Task Group methodology was to develop Best Practices by identifying and closing gaps, identifying wireless network service applicability and implementing the results of the Effectiveness Survey. The following table summarizes the results of the Best Practice work resulting from these activities. Subsequent sub-sections will provide additional details for each of the activities defined in the methodology.

Table 3.2.5.3. Payload Task Group Summary of Best Practice Activities.

	Gap Closure Process (1 Gap)	Effectiveness Survey Process	Wireless Services Applicability Improvement Process	TOTAL
New Best Practices	1	0	0	**1**
Modified Best Practices	0	0	2	**2**
Deleted Best Practices	0	0	0	**0**

3.2.5.4 Payload Gap Analysis

The Council Charter directs the Focus Group to "*perform a gap analysis to determine areas where new Best Practices for wireless networks are needed*." The approach used by the Payload Task Group was similar to the process used in other areas as described in Section 2.3.5. Therefore, a gap is here defined as a space between the known problems associated with payload that can impact network reliability and the existing Best Practices for payload. To understand the former boundary, a list was generated of 28 known concerns for payload. To understand the latter boundary, the existing Best Practices were researched and 34 were found to have potential application to the wireless network reliability.[17] In addition, the Task Group reviewed the work of the previous Council in which the vulnerabilities of payload were systematically reviewed.[18] [19]

The Task Group has identified one Gap:

Spam Control at Message Centers and MSCs

[17] The NRIC Best Practices related to bandwidth monitoring were 6-6-8074 and 6-6-8075. The NRIC Best Practices identified using the keyword "signaling" were 6-5-0517, 6-6-8040, 6-6-0770, 6-6-8040, 6-6-8051, 6-6-8052, 6-6-8053, 6-6-8054, 6-6-8060 and 6-6-8104. The NRIC Best Practices identified using the keyword "encryption" were 6-6-5062, 6-6-8001, 6-6-8006, 6-6-8012, 6-6-8013, 6-6-8025, 6-6-8028, 6-6-8029, 6-6-8049, 6-6-8051, 6-6-8052, 6-6-8059, 6-6-8060, 6-6-8091, 6-6-8094, 6-6-8096, 6-6-8105 and 6-6-8503. The keyword "interception" resulted in 6-6-5173. For bandwidth variations (e.g., Mass calling), Best Practices 6-6-0576, 6-6-8074 and 6-6-8075 were identified.

[18] The Homeland Security Physical Security Focus Group (1A) of NRIC VI carefully listed the *categories* of payload vulnerability. See NRIC VI Homeland Security Physical Security Focus Group Final Report, Issue, 3, December 2003, p. 49.

[19] Network Reliability and Interoperability Council Homeland Defense, Focus Group 1B (Cybersecurity): Summary Report and Proposals from Cybersecurity Best Practices Work Completed by FG1B Between March 2002 and March 2003.

Concerns regarding spam controls between Message Centers and MSCs need to be addressed.

3.2.5.5 Payload Gap Closure

The wireless payload gap identified in the previous section was closed with the following Best Practice:

- **7-P-0449** Network Operators and Service Providers should, where feasible, deploy spam controls in relevant nodes (e.g., message centers, email gateways) in order to protect critical network elements and services.

3.2.5.6 Payload Effectiveness Survey Process

The payload Best Practices selected for the Effectiveness Survey were rated effective or moderately effective and, as such, no modifications were identified.

3.2.5.7 Payload Services Applicability Improvement Process

The Council Charter directs the Focus Group to "*The Council shall evaluate the efficacy of all Best Practices that have been developed for the wireless industry.*" As described in Section 2.3.5, the Payload Task Group was assigned a number of areas of concerns. Each concern was systematically investigated to determine if an existing Best Practice already addressed the concern, an existing Best Practice needed to be modified to adequately address the concern or a new Best Practice needed to created. Based on the experience and expertise of the Task Group two existing Best Practices were modified.

- **7-P-1033** Network Operators should develop a strategy for deployment of emergency mobile assets such as Cell on Wheels (COWs), cellular repeaters, Switch on Wheels (SOWs), transportable satellite terminals, microwave equipment, power generators, HVAC units, etc. for emergency use or service augmentation for planned events (e.g., National Special Security Event (NSSE)).

- **7-P-0595** Service Providers and Network Operators should be aware of the dynamic nature of peak traffic periods and should consider scheduling potentially service-affecting procedures (e.g., maintenance, high risk procedures, growth activities) so as to minimize the impact on end-user services.

3.2.5.8 Payload Issues for Further Investigation

Based on scope, known processes in place, there are, for the payload area, no items identified for further investigation.

3.2.6 POLICY

3.2.6.1 Policy Subject Matter

Policy, as utilized in the eight element communications infrastructure framework, relates to any situation in which multiple entities must agree with each other – whether it be industry, government or other entities. Thus, industry standards, peering agreements, mutual aid, and regulatory or jurisdictional matters are included. The scope of this Task Group includes review of practices that involve the coordination between industry and the various governmental agencies that impact or are impacted by this industry. These agencies may include the Federal Communications Commission, the Department of Homeland Security, Department of Defense, and state and municipal utility commissions and agencies. The areas discussed pertained to existing policies that industry believed needed review as well as areas that government wished to see reviewed by industry.

3.2.6.2 Task Group Participants

The Policy Task Group assembled a team of sufficient expertise to effectively address the Policy subject matter as it relates to the reliability of wireless networks. The Policy Task Group was made up of 4 participants. In addition to members of the Focus Group, the Task Group engaged other subject matter experts to strengthen its expertise. Due to the subject matter of this Task Group, care was taken to ensure representation from government groups in addition to industry. Table 3.2.6.2 lists the Policy Task Group participants. The team had sufficient expertise to complete this activity.

Table 3.2.6.2. Policy Task Group Participants.

Name	Organization
Mitchel Ahlbaum	City of New York, DOITT
Perry Fergus	Booz Allen Hamilton (representing NCS)
William Hitchcock, ***Leader***	Sprint
Rich Moczygemba	Cingular

3.2.6.3 Policy Summary

The Policy Task Group methodology was to develop Best Practices by identifying and closing gaps, identifying wireless service applicability and implementing the results of the Effectiveness Survey. The following table summarizes the results of the Best Practices resulting from these activities. Subsequent sub-sections will provide additional details for each of the activities defined in the methodology.

Table 3.2.6.3. Policy Task Group Summary of Best Practice Activities.

	Gap Closure Process (1 Gap)	Effectiveness Survey Process	Wireless Services Applicability Improvement Process	TOTAL
New Best Practices	1	0	3	**4**
Modified Best Practices	0	0	1	**1**
Deleted Best Practices	0	0	0	**0**

3.2.6.4 Policy Gap Analysis

The Council Charter directs the Focus Group to "*… perform a gap analysis to determine areas where new wireless Best Practices are needed*." In addition, *"The Council shall focus on the special needs of the wireless industry and refine existing Best Practices to focus their applicability to the wireless industry."* The approach used by the Policy Task Group was similar to the process used in other areas as described in Section 2.3.5. Therefore, a gap is here defined as a space between the known problems associated with policy that can impact network reliability and the existing Best Practices for policy. To understand the former boundary, a list was generated of 52 known concerns for policy. To understand the latter boundary, the existing Best Practices were researched and 162 were found to have potential application to the policy issues surrounding the reliability of wireless networks. In addition, the Task Group reviewed the work of the previous Council in which policy vulnerabilities were systematically reviewed.

After thorough review of the initial 52 concerns potentially related to policy, the Task Group gave each of the items a final disposition of one of the following: transfer to another Task Group, addressed by existing Best Practice, modification to existing Best Practice, deemed out of scope of this Task Group, or gap.

The Task Group has identified the following gap:

Non-Destructive Fire Suppression

Fire suppression systems (e.g., FM200, Halon) as an equivalent alternative to water based sprinklers that could cause damage to equipment thus expanding or prolonging an outage.

3.2.6.5 Policy Gap Closure

NRIC VI identified four Best Practices[20] that are applicable to fire suppression in telecom facilities. The following new NRIC Best Practice has been defined to address the gap that was identified by the Policy Task Group.

- **7-P-0488**- Service Providers and Network Operators should consult National Fire Prevention Association Standards (e.g., NFPA 75 and 76) for guidance in the design of fire suppression systems and for zoning considerations during the planning phase of a new site.

3.2.6.6 Policy Effectiveness Survey Process

The Policy Task Group Best Practices selected for the Effectiveness Survey were rated 91% as effective or moderately effective and, as such, no modifications were required. Of the remaining 9%, the Task Group reviewed the comments from the survey and drafted proposed modifications to resolve those issues. The proposed modifications were submitted to Focus Group 2A as the specific Best Practices in question fell under their purview.

[20] Obtained via the NRIC VI Best Practice web site using text search with 'Fire Suppression.'

3.2.6.7 Policy Services Applicability Improvement Process

Per the NRIC VII charter, the Wireless Best Practices Focus Group was to “refine existing Best Practices to focus their applicability to the wireless industry.”

The Task Group was assigned issues of concern, some of which were identified as gaps in existing Best Practices (see Section 3.2.6.4). Other issues required actions to be taken to create new or modify existing Best Practices. For the Policy Task Group, most of the identified issues were addressed by existing Best Practices, however, the following revision and new Best Practices serve to augment the existing body of work to account for the special needs of the wireless industry.

- **7-P-1031** Service Providers and Network Operators should consider entering into Mutual Aid agreements with partners best able to assist them in a disaster situation using the templates provided on the NRIC and NCS websites. These efforts could include provisions to share spectrum, fiber facilities, switching, and/or technician resources.

- **7-P-0489** Service providers and Network Operators should ensure that critical wireless circuits (e.g., high priority cells, SS7 circuits, 911 circuits) are registered with TSP (Telecom Service Priority).

- **7-P-0490** Equipment Suppliers, Network Operators and Service Providers should consider provisions in labor contracts to provide for cooperation between union and non-union personnel during disaster recovery situations.

- **7-P-0491** Equipment Suppliers, Service Providers and Network Operators should, where programs exist, coordinate with local, state and/or federal emergency management and law enforcement agencies for pre-credentialing to help facilitate access by technicians.

3.2.6.8 Policy Issues for Further Investigation

Based on scope, known processes in place, there are some issues that will require further investigation by future councils.

- **Wireless Priority Service (WPS)** - As WPS is an emerging service and not currently available for all wireless technologies, the Task Group felt it was premature to try to address this area. However, as it becomes more widely implemented, it would be of benefit to identify the industry Best Practice in its management.

- **Emergency Response to Text** – The additional functionalities provided by wireless handsets such as Short Message Service (SMS) and interactive media services create alternative means of communication to emergency response channels. Consideration should be given to advanced handset capabilities and alternatives to voice communication.

3.2.7 POWER

3.2.7.1 Power Subject Matter

The power area includes the internal power systems, batteries, grounding, high voltage and other cabling, fuses, back-up emergency generators and fuel.[21] Power is an essential basic element of the communications infrastructure, without which networks will not function. In addition, any power problem has the potential to become a catastrophe, potentially damaging other equipment and personnel.[22]

3.2.7.2 Power Task Group Participants

The Power Task Group assembled a team of experts to effectively address the power subject matter as it relates to the reliability of wireless networks. The Power Task Group was made up of 5 participants. Network Operators, Power Equipment Manufacturers, and Telecommunications Equipment Manufacturers were all represented on the team. In addition, the Task Group engaged other subject matter experts to strengthen its expertise. Table 3.2.7.2 lists the Power Task Group participants. The team had the requisite expertise to complete this activity.

Table 3.2.7.2. Power Group Task Group Participants.

Name	Organization
William Hitchcock	Sprint
Richard Krock, ***Co-Leader***	Bell Labs, Lucent Technologies
John Mardula, ***Co-Leader***	T-Mobile
Leo Palumbo	AT&T
Howard Washer	Batterycorp

3.2.7.3 Power Summary

The Power Task Group methodology was to develop Best Practices by identifying and closing gaps, identifying wireless service applicability and implementing the results of the Effectiveness Survey. The following table summarizes the results of the Best Practices resulting from these activities. Subsequent sub-sections will provide additional details for each of the activities defined in the methodology.

Table 3.2.7.3. Power Task Group Summary of Best Practice Activities.

	Gap Closure Process (2 Gaps)	**Effectiveness Survey Process**	**Wireless Services Applicability Improvement Process**	**TOTAL**
New Best Practices	8	0	0	**8**
Modified Best Practices	0	0	1	**1**
Deleted Best Practices	0	0	0	**0**

[21] The communications infrastructure is also dependent on commercial energy. This commercial power is external to the communications infrastructure.

[22] NRIC VI Homeland Security Physical Security Focus Group Final Report, Issue, 3, December 2003, p. 44

3.2.7.4 Power Gap Analysis

The Council Charter directs the Focus Group to "*… perform a gap analysis to determine areas where new wireless Best Practices are needed*." In addition, *"The Council shall focus on the special needs of the wireless industry and refine existing Best Practices to focus their applicability to the wireless industry."* The approach used by the Power Task Group was similar to the process used in other areas as described in Section 2.3.5. Therefore, a gap is here defined as a space between the known problems associated with power that can impact wireless network reliability and the existing Best Practices for power. To understand the former boundary, a list was generated of 30 known concerns related specifically to electrical power in wireless networks. To understand the latter boundary, the existing Best Practices pertaining to power (approximately 100[23]) were researched and 20 of the identified concerns were found to be adequately addressed by existing Best Practices. In addition, many of the existing power Best Practices apply to various aspects of wireless networks. From the remaining 10 issues, two gaps were identified.

Emergency power for cell sites

- Emergency power for backhaul equipment as well as radio equipment.
- Plans for long term back-up power for cell sites.

Priority restoration of power to cell sites

- Critical cell sites need priority restoration of electrical power

Events during the past few years (e.g., 2003 East Coast Blackout, 2004 hurricanes) have increased the awareness of and focus on power issues in the wireless sector. As a result of these events and in addition to the work of this task group, a workshop dealing with Emergency Back-up Power for remote equipment locations was held on November 22, 2004 with broad industry support, including the electrical power industry. The Power Task Group considered the findings of that conference during their analysis of power issues.

3.2.7.5 Power Gap Closure

Long Term Back-up Power for Remote Sites

While major communications locations generally are equipped with back-up power, and numerous Best Practices talk to that issue, remote locations present a different set of challenges. Six new Best Practices were identified that deal with the unique aspects of providing back-up power to remote communications sites.

[23] 6-6-0512, 6-5-0527, 6-5-0543, 6-5-0544, 6-5-0622, 6-5-0623, 6-5-0624, 6-5-0625, 6-5-0627, 6-5-0634, 6-5-0635, 6-5-0636, 6-5-0637, 6-5-0638, 6-5-0642, 6-5-0644, 6-5-0648, 6-5-0650, 6-5-0651, 6-5-0652, 6-5-0653, 6-5-0654, 6-6-0655, 6-5-0656, 6-5-0657, 6-5-0658, 6-5-0659, 6-5-0660, 6-5-0661, 6-5-0662, 6-5-0663, 6-5-0664, 6-5-0665, 6-5-0666, 6-5-0667, 6-5-0668, 6-5-0669, 6-5-0670, 6-5-0671, 6-5-0672, 6-5-0673, 6-5-0674, 6-5-0675, 6-5-0676, 6-5-0677, 6-5-0678, 6-5-0679, 6-5-0680, 6-5-0681, 6-5-0682, 6-5-0683, 6-5-0684, 6-5-0685, 6-5-0687, 6-5-0688, 6-5-0689, 6-5-0690, 6-5-0691, 6-5-0692, 6-5-0693, 6-5-0694, 6-5-0695, 6-5-0696, 6-5-0697, 6-5-0698, 6-5-0699, 6-5-0700, 6-5-0701, 6-5-0702, 6-5-0703, 6-6-0760, 6-6-0761, 6-6-1027, 6-6-1028, 6-6-1029, 6-6-1030, 6-6-1067, 6-6-5041, 6-6-5042, 6-6-5058, 6-6-5073, 6-6-5076, 6-6-5197, 6-6-5203, 6-6-5204, 6-6-5205, 6-6-5206, 6-6-5207, 6-6-5208, 6-6-5209, 6-6-5210, 6-6-5211, 6-6-5212, 6-6-5213, 6-6-5214, 6-6-5216, 6-6-5231, 6-6-5232, 6-6-5241, 6-6-5275, 6-P-5281

- **7-P-0492** Network Operators should provide back-up power (e.g., some combination of batteries, generator, fuel cells) at cell sites and remote equipment locations, consistent with the site specific constraints, criticality of the site, the expected load and reliability of primary power.

- **7-P-0493** Network Operators and Property Managers should consider placing fixed power generators at cell sites, where feasible.

- **7-P-0493** Network Operators and Property Managers should consider including a provision in cell-site contracts for back-up power.

- **7-P-0496** Network Operators and Property Managers should consider storing their portable generators at critical sites that are not otherwise equipped with stationary generators.

- **7-P-0497** Network Operators and Property Managers should consider connecting the power load to portable generators where they are stored, and configuring them for auto-engage in the event of a failover.

- **7-P-0498** Network Operators and Property Managers should consider alternative measures for cooling network equipment facilities (e.g., powering HVAC on generator, deploying mobile HVAC units) in the event of a power outage.

Restoration of commercial electric power

The numerous equipment locations associated with providing wireless service compound the problem of obtaining rapid restoration of commercial power following a failure. This was confirmed during the Emergency Back-up Power Workshop. Existing Best Practices touch on programs such as Telecommunications Electric Service Priority (TESP), but an additional Best Practice was identified to improve the speed of power restoration to remote sites.

- **7-P-0495** Network Operators and Property Managers should consider pre-arranging contact information and access to restoral information with local power companies.

Power for back-haul equipment

The value of providing back-up power to cell sites is greatly diminished if the facility equipment used to provide back-haul at the cell site is not also provided with back-up power. A new Best Practice was identified to address this issue.

- **7-P-0499** Network Operators and Service Providers should consider ensuring that the back-haul facility equipment located at the cell site is provided with backup power duration equal to that provided for the other equipment at the cell site.

3.2.7.6 Power Effectiveness Survey Process

The Power Best Practices selected for the Effectiveness Survey were rated as 99% effective or moderately effective and, as such, no modifications were identified.

3.2.7.7 Power Services Applicability Improvement Process

Per the NRIC VII charter, the Wireless Focus Group was to "refine existing Best Practices to improve their applicability to the wireless industry."

The Task Group was assigned issues of concern, some of which were identified as gaps in existing Best Practices (see Section 3.2.7.4). Other issues required actions to be taken to create new or modify existing Best Practices. The Power Task Group recommended additional wording to one existing Best Practice to improve the applicability to the wireless industry.

- **6-6-1028 -** Service Providers and Network Operators should engage in preventative maintenance programs for network site support systems including emergency power generators, UPS, DC plant (including batteries), HVAC units, and fire suppression systems.

3.2.7.8 Power Issues for Further Investigation

Based on scope and known processes in place, there are no power items identified for further investigation.

3.2.8 SOFTWARE

3.2.8.1 Software Subject Matter

Software is a critical component when addressing the overall reliability of wireless networks. Software is a factor relative to its own reliability as well as in the ability to enhance the resilience of the network when other conditions might otherwise jeopardize the network.

When considering software issues in the context of network reliability, software includes operating systems, application code, protocols, configuration and subscriber usage data. Such software may reside on a network switching or radio access element or on an application server. Software may be contained on a variety of mediums inclusive of volatile/non-volatile memory, magnetic or optical disc, magnetic tape, or other storage technologies.

The Task Group focused on the identified concerns related to the software in wireless networks.

3.2.8.2 Software Task Group Participants

The Software Task Group assembled a team of broad expertise to effectively address the Software subject matter as it relates to the reliability of wireless networks. Table 3.2.8.2 lists the Software Task Group participants.

Table 3.2.8.2. Software Task Group Participants.

Name	Organization
Bentley Alexander, **Leader**	Ericsson
Srinivasa Anam	Nortel
John Bassett	Motorola
Slawek Deja	Nokia
Rick Krock	Bell Labs, Lucent Technologies
Brad McManus	Sprint
Vijay Patel	T-Mobile
Sherman Phillips	Qwest
Robin Roberts	Cisco

3.2.8.3 Software Summary

The Software Task Group methodology was to develop Best Practices by identifying and closing gaps, identifying wireless service applicability and implementing the results of the Effectiveness Survey. The following table summarizes the results to the Best Practices resulting from these activities. Subsequent sub-sections will provide additional details for each of the activities defined in the methodology.

Table 3.2.8.3. Software Task Group Summary of Best Practice Activities.

	Gap Closure Process (1 Gap)	Effectiveness Survey Process	Wireless Services Applicability Improvement Process	TOTAL
New Best Practices	0	0	0	**0**
Modified Best Practices	2	4	2	**8**
Deleted Best Practices	0	0	0	**0**

3.2.8.4 Software Gap Analysis

The Council Charter directs the Focus Group to "…perform a gap analysis to determine areas where new Best Practices for Wireless Network Operators, Service Providers, and Equipment Suppliers are needed." The approach used by the Software Task Group was similar to the process used in other areas as described in Section 2.3.5.

For the Software Task Group, 22 known issues involving software were identified and reviewed. The issues generally fell into one of five categories:

1. Enhancing traffic overload/capacity handling capability
2. Improving software quality in the operating environment
3. Eliminating impacts from software changes, patches, upgrades
4. Ensuring security from intentional and unintentional threats
5. Improving ability and time to restore a platform

Gaps were then identified by assessing the known issues against documented Best Practices involving software. A review of the documented Best Practices revealed 63 practices pertaining to software and the relevance to network reliability.[24]

3.2.8.5 Software Gap Closure

The Task Group's gap analysis identified one issue exposing a gap for which no applicable Best Practice was found.

Issue: The increasing opportunity for spam (undesirable messages) in wireless data networks negatively impacting network performance.

The Task Group, accordingly, proposed the following new Best Practice:

- **7-P-0449** Network Operators and Service Providers should, where feasible, deploy spam controls in relevant nodes (e.g., message centers, email gateways) in order to protect critical network elements and services.
  - Note: counted in payload section

[24] 6-5-0523, 6-5-0535, 6-5-0536, 6-5-0538, 6-5-0539, 6-5-0541, 6-5-0542, 6-5-0550, 6-5-0552, 6-5-0553, 6-5-0554, 6-5-0555, 6-5-0557, 6-5-0559, 6-5-0565, 6-6-0575, 6-5-0590, 6-5-0600, 6-5-0601, 6-5-0745, 6-5-0749, 6-5-0750, 6-6-0762, 6-6-0763, 6-6-0764, 6-6-0765, 6-6-0766, 6-6-0767, 6-6-0768, 6-6-0769, 6-6-0770, 6-6-0802, 6-6-1034, 6-6-5004, 6-6-5061, 6-6-5084, 6-6-5121, 6-6-5142, 6-6-5165, 6-6-5166, 6-6-5167, 6-6-5170, 6-6-5171, 6-6-5172, 6-6-5200, 6-6-5218, 6-6-5219, 6-6-5254, 6-6-5277, 6-6-5278, 6-6-5279, 6-6-8003, 6-6-8010, 6-6-8027, 6-6-8033, 6-6-8034, 6-6-8035, 6-6-8074, 6-6-8094, 6-6-8096, 6-6-8100, 6-6-8103, 6-6-8527

The remaining identified issues were addressed by previously documented Best Practices or were capable of being addressed by making a slight revision to an existing Best Practice. Those Best Practices requiring revision are shown below with the proposed text:

- **7-P-0559** Service Providers and Network Operators should consider validating upgrades, new procedures and commands in a lab or other test environment that simulates the target network and load prior to the first application in the field.

- **7-P-0745** Equipment Suppliers should design equipment so that initializations or upgrades of hardware or software are implemented with minimal or no service impact.
    - Note: This Best Practice will be reviewed by a Joint 2A/3A session prior to 2A's final report.

3.2.8.6 Software Effectiveness Survey Process

The Software Best Practices selected for the Effectiveness Survey were scored as 98% being effective or moderately effective and only 2% as non-effective. The primary issue cited as limiting the effectiveness of the particular Best Practices was that multiple practices were included under a single practice entry. Accordingly, the subject practices were modified to result in separate and distinct practices as shown below.

- **7-P-0600** Service Providers and Network Operators should establish and document a process to plan, test, evaluate and implement major change activities onto their network.

- **7-P-0447** Service Providers and Network Operators should consider establishing a customer advocacy group to take part in the development and scheduling of changes in order to minimize impact.

- **7-P-0750** Equipment Suppliers should provide a mechanism for feature activation or deactivation that is not service impacting to end-users. For example, avoid re-boot, re-start or re-initialization.

- **7-P-0448** Equipment Suppliers should, where feasible, provide a memory management capability to reconfigure or expand memory without impacting stable calls or other critical processes (e.g., billing).

3.2.8.7 Software Services Applicability Improvement Process

Per the NRIC VII charter, the Wireless Network Reliability Focus Group was to "refine existing Best Practices to focus their applicability to the wireless industry."

Two existing Best Practices were modified to be more inclusive of wireless networks. The revised practices are shown below:

- **7-P-0517 Equipment Control Mechanisms:** Equipment Suppliers should design network elements and associated network management elements with the combined capability to dynamically handle peak load and overload conditions gracefully and queue and/or shed traffic as necessary (e.g., flow control).

- **7-P-0603 Schedule System Backups:** Service Providers should establish policies and procedures that outline how critical network element databases will be backed up onto a storage medium (e.g., tape, optical diskettes) on a scheduled basis.

3.2.8.8 Software Issues for Further Investigation

One issue that was identified as a possible gap but determined to be outside the scope of this Focus Group is the issue of manageability of third- party applications for wireless devices and handsets. Given the proliferation of content and media for wireless fixed, mobile, and handheld devices in today's voice and data networks, there are an unending number of practices that can be defined for the software development, implementation, and application management of these devices. However, in the context of Network Reliability, this Task Force determined it was appropriate to limit scope to the ability of a handset to conduct basic communications and thus did not address any gaps relative to third party wireless software applications.

3.3 Survey of Effectiveness

This section describes how the Focus Group fulfilled the requirement in its mission to conduct an industry survey on the effectiveness of existing Best Practices. Specifically, the NRIC VII Charter directs the Council to "… survey providers of wireless network services, including Internet data services providers, concerning the efficacy of existing Best Practices." The Charter further directs that "By April 29, 2005, the Council shall complete its survey of the effectiveness of the Best Practices for Internet data services."

3.3.1 Additional Industry Engagement

Getting an outside perspective is one of the principles of developing Best Practices.[25] Conducting industry surveys of Best Practices has been part of several previous Councils. While NRIC focus groups typically have broad representation, these surveys usually extend to even a wider reach. For example, some companies may not have the resources to participate in the monthly meetings. However, the survey is a way for their perspective to be included in the process.

3.3.2 Use of Third Party

Because information collected on Best Practices from an individual company may be sensitive, the Focus Group elected to employ a trusted, third party entity to assist in conducting the survey. With the guidance of the Charter, the Focus Group prioritized the following criteria in its Request for Proposal (RFP) process:

- Approach to supplying the services sought
- Demonstrated organizational capability
- Qualifications of personnel
- Price

Since the Public Data Network Focus Group (3B), had a similar survey requirement in its mission, the selection process was coordinated across the two Focus Groups. The joint Focus Group evaluation process resulted in the selection of BPI-Telcodata[26] to conduct this industry survey.

3.3.3 Timeline

The survey was completed between December, 2004 and March, 2005. The larger timeline can be summarized as follows:

- December 2004 – charter interpretation, RFP development, RFP outreach, RFP response analysis
- January 2005 – field test, commencement of survey
- February 2005 – completion of survey
- March 2005 – analysis of results
- April – June 2005 – Best Practice adjustments based on learnings

[25] Section 3.3.2, Principle 6

[26] BPI-Telcodata is an independent consulting firm that provides benchmarking and best practice consulting, regulatory support, demand analysis and forecasting, survey and database services for carriers and vendors on many areas including service reliability, cost analysis, market planning and other performance metrics. www.telcodata.net

3.3.4 Approach

There are hundreds of Best Practices that apply to the reliability of wireless networks. In order to have a survey that respondents could complete in a reasonable amount of time, the number of Best Practices could not be too large. Therefore, the Focus Group selected representative Best Practices from each of the eight areas of communications infrastructure: Environment, Hardware, Human, Network, Payload, Policy, Power and Software. The respective Task Group leaders and subject matter experts selected ten Best Practices that best represented each of these areas. The number of Best Practices selected represented approximately a quarter of those applicable.

This survey was designed to catalog and analyze the opinions of Service Providers, Network Operators and Equipment Suppliers regarding the effectiveness of Best Practices. Four questionnaires were fielded, two for Service Providers and Network Operators (Wireless and Public Data Network) and two for Equipment Suppliers (Wireless and Public Data Network).[27] The respondents rated each Best Practice's effectiveness on network reliability.[28] Respondents were also given the opportunity to provide comments and other feedback on each Best Practice.

BPI-Telcodata designed and distributed the questionnaires, collected and tabulated the responses, and produced detailed reports with tables, graphs and respondent commentaries. All of the responses were treated as proprietary information and careful security measures were used to ensure that, whereas no response could be linked to any company, the information obtained from the surveys could be used to generate aggregate summaries.

This survey had the highest number of respondents ever for an NRIC survey (Figure 3.3.4). The combined Focus Group 3A and Focus Group 3B respondents was 38.

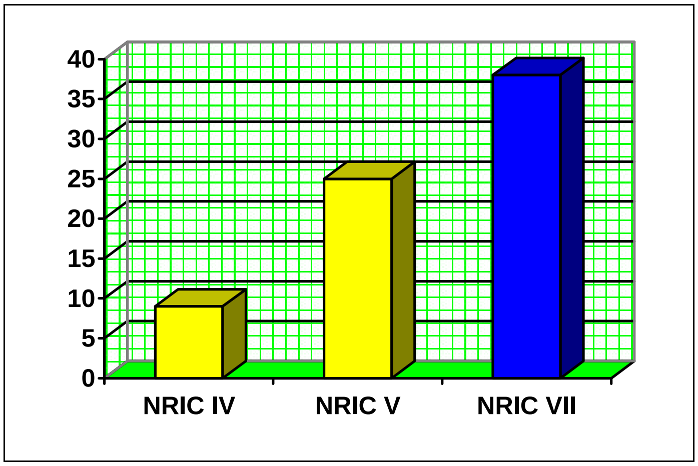


Figure 3.3.4. Improvement in Number of Survey Respondents

[27] The number of Best Practices in each survey was as follows: Service Provider and Network Operator - Wireless (65), PDN (67); Equipment Supplier – Wireless (42), PDN (38)

[28] For each Best Practice, respondents could select from the following choices: Effective, Moderately Effective, Not Effective, Don't Know, and Not Applicable.

The number of survey responses in NRIC VII for both the wireless and public data network companies was sufficiently large to support the statistical results and assessments that were reported. The results provide useful information on the distribution of Best Practice responses, on the grouping and comparison of Best Practices and on the assessment of Best Practices by respondent category (e.g., wireless, public data network service providers). The participating companies were representative of the industry. Significant inroads were made in recruiting firms that were not NRIC members.

Of the survey participants, those that are wireless network service providers or network operators represent:

- Over 92% of the switched lines in-service in the US.
- Over 95% of the domestic wireline local, access and toll revenues.
- Approximately 95% the circuit switches in-service in the US.
- Over 94% of the core routers shipped domestically

3.3.5 Survey Results

The survey results are summarized in Table 3.3.5 below. The detailed adjustments from the learnings for each Best Practice are reported in the individual Task Group sections (Sections 3.2.1 to 3.2.8). Best Practices classified as "Ineffective" were reviewed by the Task Groups and either modified or deleted based on the comments received.

Table 3.3.5. Survey Results.

Number of Participants[29]	38
Number of Best Practices Surveyed	80
% of Best Practices Rated as Effective or Moderately Effective on Average	97%

3.3.6 Other Observations

There are two additional observations worth mentioning. The first is that the survey results indicated there was strong agreement for those Best Practices rated as "Effective" (i.e., those that received this highest rating often did so by nearly everyone).

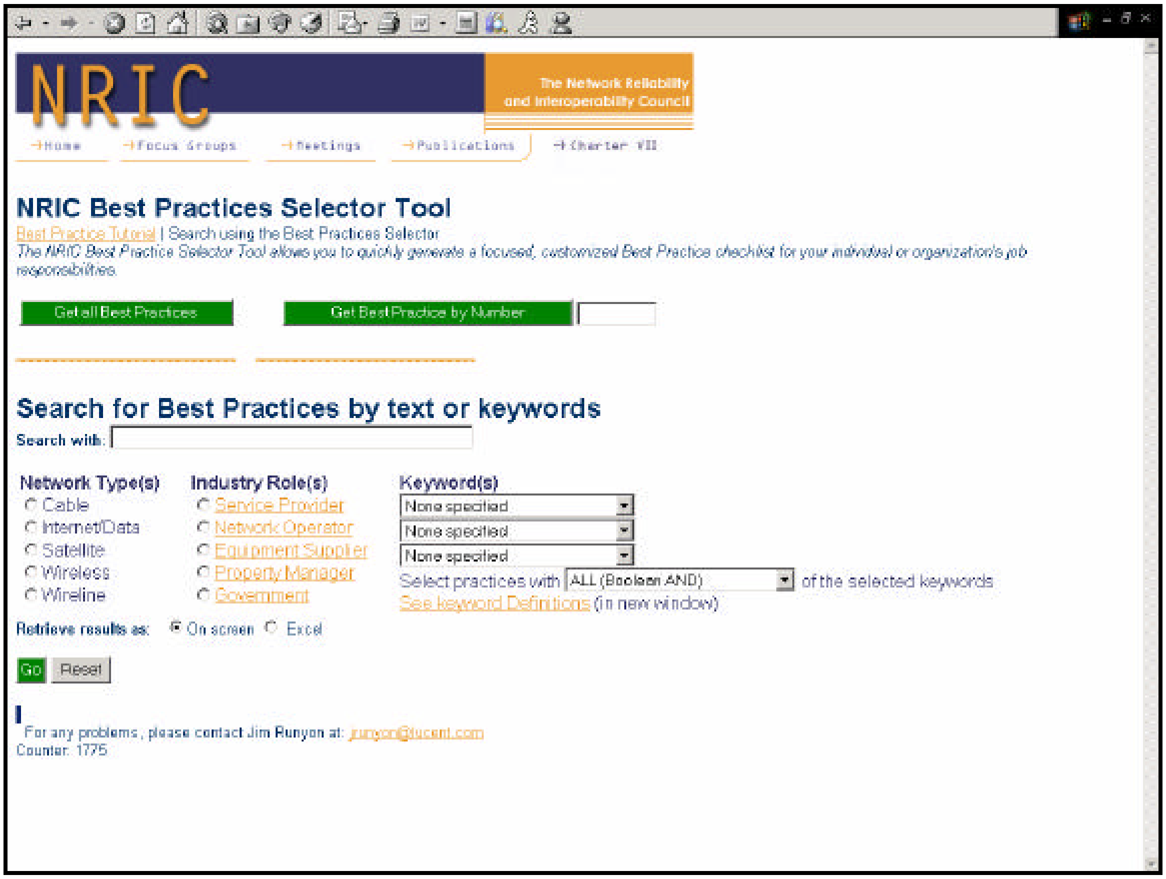
The second observation is that some Best Practices are identified by subject matter experts as being effective, and by other experts as being not applicable. This survey evidence further supports the principle that Best Practices are not applicable in all situations, as is stated throughout this report.

[29] For comparative purposes, represents the combined Focus Group 3A and Focus Group 3B survey; this represents a 52% improvement over NRIC V industry participation.

3.4 Best Practices

This section provides additional details on NRIC Best Practices that supplement the discussed in Section 2.3.2.

The NRIC Best Practices are maintained on the NRIC web site (www.nric.org). The NRIC Best Practice search page is shown below:



NRIC Best Practices Selector Tool

Best Practice Tutorial | Search using the Best Practices Selector

The NRIC Best Practice Selector Tool allows you to quickly generate a focused, customized Best Practice checklist for your individual or organization's job responsibilities.

Search for Best Practices by text or keywords

Search with:

Network Type(s)	Industry Role(s)	Keyword(s)
○ Cable	○ Service Provider	None specified
○ Internet/Data	○ Network Operator	None specified
○ Satellite	○ Equipment Supplier	None specified
○ Wireless	○ Property Manager	Select practices with ALL (Boolean AND) of the selected keywords
○ Wireline	○ Government	See keyword Definitions (in new window)

Retrieve results as: ● On screen ○ Excel

For any problems, please contact Jim Runyon at: jrunyon@lucent.com
Counter: 1775

Figure 3.4. NRIC Best Practices Selector Tool.

This web site provides a flexible means to retrieve NRIC Best Practices. The Best Practice selection options include:

- Selecting all Best Practices
- Selecting a specific Best Practice by number
- Searching for Best Practices containing a specified text
- Selecting Best Practices for Network Types (e.g., wireless networks)
- Selecting Best Practices based on Industry Roles (e.g., Service Provider)
- Selection using one to three Keywords

The following subsection provide a perspective on NRIC Best Practices developed by previous NRIC Councils, describes the intended use of Best Practices, describes the search options for the Best Practices, the methodology used to define Best Practices, and the Best Practice numbering scheme.

3.4.1 Best Practices and Previous Councils

Previous Councils provided Best Practices for the industry throughout their Final Reports. The earlier Councils focused on network reliability with particular attention to signaling and essential services; later Councils focused on interoperability. With the growing appreciation for their value in subsequent Councils, the Best Practices were increasingly drawn out of the reports as a distinct list. Also, the more recent Councils' scope for Best Practices expanded from traditional circuit switched technologies in wireline networks to wireless, cable and satellite networks as well as packet switched and converged solutions technologies.

The effectiveness of the NRIC Best Practices in preventing outages has been demonstrated consistently over the years. The ATIS NRSC has pointed out in its reports that most outages monitored at the national level could have been prevented if existing NRIC Best Practices had been implemented[30]. A thorough industry survey of the industry's implementation of NRIC V Best Practices was conducted in the second half of 2001. The results were reported in the NRIC V Network Reliability Best Practices Subcommittee Final Report. The results of this survey provide valuable insights into several dimensions of the industry's view of these Best Practices. The fifth Council noted the following key learning's regarding the network reliability Best Practices from analysis of the industry survey:

- There is moderate to high risk to <u>not</u> implement the Best Practices
- There is usually **not** a high cost to implement the Best Practices
- The Best Practices are effective in preventing outages
- There is already a high level of implementation of the Best Practices[31]

3.4.2 Intended Use

Service Providers, Network Operations, and Equipment Suppliers are encouraged to prioritize their review of these Best Practices and prioritize their implementation, as appropriate.

As noted elsewhere in this report, the appropriate application of these Best Practices can only be done by individuals with sufficient knowledge of company specific network infrastructure architecture to understand their implications. Although the Best Practices are written to be easily understood, their meaning is often *not* apparent to those lacking this prerequisite knowledge and experience.

The NRIC Best Practices are intended to give guidance on how best to protect the U.S. communications infrastructure. Decisions of whether or not to implement a specific Best Practice are intended to be left with the responsible organization (e.g., Service Provider, Network Operator, or Equipment Supplier). Mandated implementation of these Best Practices is *not* consistent with their intent. As noted elsewhere in this report, the

[30] NRSC Quarterly and Annual Reports provide detailed analyses of the industry's outage trends. The NRSC analysis of major network outages provides an understanding of the direct and root causes. These reports consistently find that existing NRIC Best Practices, if implemented, would prevent most of the major outages. www.atis.org

[31] Network Reliability Best Practices Subcommittee (2A.2) Presentation to the NRIC V Council and FCC at the FCC Building, January 4, 2002. www.nric.org.

appropriate application of these Best Practices can only be done by individuals with sufficient knowledge of company specific network infrastructure architecture to understand their implications. Although the Best Practices are written to be easily understood, their meaning is often *not* apparent to those lacking this prerequisite knowledge and experience. Appropriate application requires understanding of the Best Practice impact on systems, processes, organizations, networks, subscribers, business operations, complex cost issues and other considerations. With these important considerations regarding intended use, the industry stakeholders are concerned that government authorities may inappropriately impose these as regulations or court orders. Because the NRIC Best Practices have been developed as a result of broad industry cooperation that engages vast expertise and considerable voluntary resources, such misuse of these Best Practices may jeopardize the industry's willingness to work together to provide such guidance in the future.

These Best Practices continue the theme stated over 10 years ago in the first NRIC (NRC) Report "Network Reliability: A Report to the Nation", also known as "The Purple Book").

> **"The Best Practices, while not industry requirements or standards, are highly recommended. The First Council stated, 'Not every recommendation will be appropriate for every company in every circumstance, but taken as a whole, the Council expects that these findings and recommendations [when implemented] will sustain and continuously improve network reliability.' "**[32]

The NRIC Best Practices continue to be developed consistent with this historic precedent.

3.4.3 Best Practice Search Options

3.4.3.1 Industry Roles

Each Best Practice can have associations with any combination of five industry roles:

- Service Providers
- Network Operators
- Equipment Suppliers
- Government
- Property Manger

3.4.3.2 Network Types

Each Best Practices is also associated with one of the following network types:

- Cable
- Internet/Data
- Satellite
- Wireless
- Wireline

[32] Executive Summary, NRIC V Best Practices Subcommittee Final Report, January 2002

3.4.3.3 Keywords

Keywords are not provided for every possible category that relates to Best Practices, but rather are provided to be as a means of helping the many users determine which Best Practices apply to their job responsibilities.

3.4.4 General, Previous Council and Historic References

The material in this section borrows heavily from the NRIC V Network Reliability Best Practices Subcommittee Report.

References can be a very important research tool for a user to determine applicability. References have been organized into three types:

- General
- Previous Council
- Historic

General references include citations or Web links to industry standards, white papers, or any other useful documentation. Previous Council references consist of the NRC I, NRC II, NRIC III, NRIC IV and NRIC V Final Reports. Historic references include specific examples of outages (e.g., the 1988 Hinsdale Fire) that provide insights into how neglecting the associated Best Practice could have a substantial negative impact. Such information can be very important to a user considering the applicability of a set of Best Practices.

This organizational structure of references has proven useful and is expected to provide better management of the insertion of future references.

This capability provides substantial value to the users and is expected to result in ever increasing levels of implementation of Best Practices.

3.4.5 Best Practices Expressions

3.4.5.1 Basic Form

Most Best Practices have at their core a simple statement of the form:

"____ should _____, "

Where the first blank consists of any combination of Service Provider, Network Operator, Equipment Supplier, Property Manager, and Government, the second blank consists of the basic practice.

Such Best Practice sentences may be augmented with an "in order to . . ." statement that provides clarity as to the intent of the suggested action(s). This information may also be accessed, when available, on the web site.

There are also situations where the industry experts are aware that they are able to give very valuable guidance to the industry, but at the same time realize that the guidance would not fit every situation. The broad industry expertise often recognized that the vast diversity of networks and special conditions required some expression of understanding so as to not frustrate users of the Best Practices. In articulating the Best Practices, consistent with the work completed under previous Councils, the Focus Group met both objectives of (1) providing the valuable guidance, and (2) anticipating the diversity of circumstances, by using the following expressions to represent the flexibility needed by the industry:

“Should Consider”
This expression indicates that the subject should receive the guidance offered, but that implementation should be done only after carefully thinking through the benefits along with other considerations.

“As Appropriate, or When Appropriate, or Where Appropriate”
This expression indicates that the other factors need to be considered.

“When Feasible or Where Feasible”
This expression is similar to “As Appropriate”, except that it emphasizes the business or financial factors.

3.4.5.2 Critical Communications Infrastructure Facilities

Some Best Practices are intended for critical communications infrastructure. Because of the complex, sensitive and proprietary nature of this subject, critical communications infrastructure is defined by its owners and operators. Generally, such distinction applies to points of concentration, facilities supporting high traffic, and network control and operations centers, and equipment supplier technical support centers.

3.4.5.3 Numbering Format

Each NRIC Best Practice has a unique number that follows the numbering format:

X - Y - Z # # #

Where,
X = the current, or most recent, NRIC Council (i.e., 7 in 2004-2005)
Y = the Council in which the Best Practice was last edited (i.e., 7 for current work)
Z = 0-4 for Network Reliability (including Disaster Recovery & Public Safety)
= 5 for Physical Security
= 8 for Cyber Security
# # = any digits, where every Best Practice has a unique Z # # #.

4 Conclusions

The Charter of the Seventh Council dedicated part of its focus to Network Reliability included a focus on wireless networks. The three deliverables identified by the NRIC VII charter were:

1. Identify gaps in existing, documented, NRIC Best Practices for the reliability of wireless networks.
2. Conduct an industry survey on the effectiveness of these Best Practices.
3. Modify existing Best Practices, and develop new Best Practices to address the specific needs of wireless networks.

4.1 Gap Analysis

The 12 gaps identified by this Focus Group were distributed across the infrastructure areas as follows:

Table 4.1. Distribution of Identified Gaps.

Area	Number of Gaps
Environment	2
Hardware	0
Human	2
Network	3
Payload	1
Policy	1
Power	2
Software	1

4.2 Effectiveness Survey

The Effectiveness Survey was completed on schedule. The following statistics summarize the survey results:

- 52% increase in the number of survey respondents (compared to NRIC V survey)
- 97% of Best Practices surveyed were rated as effective or moderately effective on average

In its analysis, the Focus Group observed that some Best Practices are identified by subject matter experts as being effective, and by other experts as being not applicable. This survey evidence further supports the principle that Best Practices are not applicable in all situations, as is stated throughout this report.

4.3 Wireless Network Best Practices

The number of new, modified or deleted Best Practices is identified in the following table.

Table 4.3 Focus Group 3A Wireless Network Summary of Best Practice Activities.

	Gap Closure Process (11 Gaps)	Effectiveness Survey Process	PDN Services Applicability Improvement Process	TOTAL
New Best Practices	43	0	8	**51**
Modified Best Practices	5	8	9	**22**
Deleted Best Practices	0	0	0	**0**

4.4 Areas for Further Investigation

In addition to completing the deliverables directed by the Council Charter, the Focus Group reviewed its work to determine if there were any discoveries that went beyond its scope, but that were appropriate to present. Three such items were identified. The Policy Task Group identified the following issues: Wireless Priority Service (WPS) and emergency response to text. The Software Task Group identified handset content and third party software applications.

- **Wireless Priority Service (WPS)** - As WPS is an emerging service and not currently available for all wireless technologies, the Task Group felt it was premature to try to address this area. However, as it becomes more widely implemented, it would be of benefit to identify the industry Best Practice in its management. [Section 3.2.6.8].

- **Emergency Response to Text** – The additional functionalities provided by wireless handsets such as Short Message Service (SMS) and interactive media services create alternative means of communication to emergency response channels. Consideration should be given to advanced handset capabilities and alternatives to voice communication. . [Section 3.2.6.8].

- **Handset Content and Third Party Wireless Software Applications** - One issue that was identified as a possible gap but determined to be outside the scope of this Focus Group is the issue of manageability of third- party applications for wireless devices and handsets. Given the proliferation of content and media for wireless fixed, mobile, and handheld devices in today's voice and data networks, there are an unending number of practices that can be defined for the software development, implementation, and application management of these devices. However, in the context of Network Reliability, this Task Force determined it was appropriate to limit scope to the ability of a handset to conduct basic communications and thus did not address any gaps relative to third party wireless software applications. . [Section 3.2.8.8].

4.5 Summary

The Focus Group completed all deliverables on time and consistent with the direction of the Council Charter. This report documents highly valuable guidance for Service

Providers, Network Operators and Equipment Suppliers that promote the reliability for the nation's wireless networks.

5 Recommendations

Industry members are encouraged to continue their strong support to ensure sufficient expertise and resources are devoted to this task and the FCC is encouraged to provide a healthy, non-regulatory environment where industry experts can come together and develop Best Practices for voluntary implementation.

Going forward, industry participants are strongly encouraged to have their respective subject matter experts review these Best Practices for applicability. The NRIC web site (www.nric.org) Best Practices tools have keyword and other search capabilities that make identifying the list of applicable Best Practices to a given job function efficient. It is critical to note that Best Practices are not applicable in every situation because of multiple factors. Therefore, government entities are cautioned that mandating Best Practices could contribute to suboptimal network reliability or result in other negative consequences.

With this understanding, the Focus Group has prepared the following recommendation for the Council to advance these Best Practices:

> **The Council recommends that the NRIC VII Wireless Network Reliability Best Practices be implemented, as appropriate, by Service Providers, Network Operators, Equipment Suppliers, and Property Managers in order to promote the reliability and robustness of the wireless networks throughout the United States.**

These Best Practices have been developed to assure optimal reliability and robustness under reasonably foreseeable circumstances. The scope of this activity also encompasses guidance that promotes the sustainability of communications networks throughout the United States; the availability of adequate communications capacity during events or periods of exceptional stress due to natural disaster, terrorist attacks or similar occurrences; and the rapid restoration of communications services in the event of widespread or major disruptions in the provision of communications services.

Appendix 1. List of Interviewees

Name	Company	ENVIRONMENT	HARDWARE	HUMAN	NETWORK	PAYLOAD	POLICY	POWER	SOFTWARE
Steven J. Paton	ALLTEL				X				
Ted Abrams	American Tower Corp.	X							
Julie Briggs	AT&T	X							
Leo Palumbo	AT&T	X						X	
Linda Ferro	AT&T	X							
Ralph Collipi	AT&T	X							
Victor DeVito, ***Lead***	AT&T	L							
Eric Hounchell	Battery Corp	X							
Howard Washer	Batterycorp							X	
Anil Macwan	Lucent Technologies			X					
Jim Runyon, ***Lead***	Lucent Technologies	X			X	L			
Karl Rauscher	Lucent Technologies					X			
Richard Krock, ***Co-Lead***	Lucent Technologies		X	X				C	X
Perry Fergus	Booz Allen Hamilton						X		
Rich Moczygemba	Cingular						X		
Robin Roberts	Cisco Systems		X						X
Mitchel Ahlbaum	City of New York, DOITT						X		
Mark Adams	Cox Communications				X	X			
Bentley Alexander, **Lead**	Ericsson		X						
Mike Sheffield	MCI					X			
John Bassett, ***Co -Lead***	Motorola		C						X
Lester Buczek, ***Co -Lead***	Motorola		C						
David Proffer	Nextel			X		X			
Slawek Deja	Nokia								X
Srinivasa Anam	Nortel				X				X
Sherman Phillips	Qwest				X				X
John Chapa	SBC	X							
Brad McManus, ***Lead***	Sprint				L				X
John Quigley, ***Lead***	Sprint			L					
Sunil Bhojwani	Sprint					X			
William Hitchcock, ***Lead***	Sprint			X			L	X	
John Mardula, ***Co-Lead***	T-Mobile							C	
Miles Schreiner	T-Mobile	X							
Vijay Patel	T-Mobile								X

Appendix 2. Bibliography and Documentation

American National Standards Institute (ANSI): http://www.ansi.org/

ATIS Network Reliability Steering Committee (NRSC): http://www.atis.org

ATIS T1.320-1999 Central Office and Similar Facilities HEMP Standard.

ATIS T1.328-2000 Protection of Telecommunications Links, Baseline Standard

ATIS T1.333-19999 Above-Baseline Protection of Telecommunications Links.

ATIS T1E1.7 Baseline Electrical Protection for Towers and Bonding and Grounding for Commercial Buildings that House PSN Equipment.

ATIS T1E1.7 Physical Protection Standard for a Universal Telecommunications Equipment Mounting Frame for Central Offices.

CERT® Coordination Center (CERT/CC) for Internet Security: http://www.cert.org/advisories/CA-1998-01.html

CFR Title 47, Vol. 5, Part 215 (Assigns NCS responsibility as Federal lead on EMP technical data and studies relating to telecommunications).

CTIA Semi-Annual Wireless Survey, June 2004
http://www.ctia.org

Federal Communications Commission Code of Federal Regulations 47, 63.100.: http://www.fcc.gov

Hurst, N.W.; Immediate and underlying causes of vessel failures; Implications for including management and organizational factors in quantified risk assessment, Paper presented at IChemE Symposium Series No. 124, Institute of Chemical Engineers, Rugby, UK.

IEEE CQR, “Proceedings of the IEEE Technical Committee on Communications Quality & Reliability (CQR) 2001 International Workshop."

Internet Engineering Task Force (IETF): http://www.ietf.org

Internet Operators (IOPS): http://www.iops.org

Network Interconnection Interoperability Forum (NIIF): http://www.atis.org

North American Network Operators' Group (NANOG): http://www.nanog.org

National Communications System (NCS): http://www.ncs.gov

NRC I Report: Network Reliability: A Report to the Nation. Alliance for Telecommunications Industry Solution (ATIS), Washington, D.C. http://www.nric.org/pubs/index.html

NRC I "Network Reliability: A Report to the Nation", Alliance for Telecommunications Industry Solutions (ATIS), Washington, D.C. http://www.nric.org/pubs/index.html

NRC II Report: "Network Reliability – The Path Forward," ATIS, February, 1996, Washington, D.C. http://www.nric.org/pubs/index.html

NRIC III Report: "NRIC Network Interoperability: The Key to Competition," ATIS, July, 1997, Washington, D.C. http://www.nric.org/pubs/index.html

NRIC IV Final Report: http://www.nric.org/fg/index2.html

NRIC V Report, "The Future of our Nation's Communications Infrastructure: A Report to the Nation," January 4, 2002: http://www.nric.org

NRIC V Best Practices web site: http://www.nric.org

NRIC VI Best Practices web site: http://www/nric.org

Network Reliability Steering Committee (NRSC) Annual Reports: www.atis.org

Pat-Cornell, M.E., & Bea, R.G.; Management Errors and System Reliability: A probabilistic approach and application to offshore platforms, Risk Analysis, vol. 12, pp. 1 - 8, 1992.

T1 Standards Committee: http://www.nric.org

T1A1 Telecom Glossary: http://www.its.bldrdoc.gov/projects/telecomglossary2000

Telcordia Generic Requirements and Technical References: http://www.telcordia.com

Telcordia Generic Requirements (GR-63) - Network Equipment-Building System (NEBS) Requirements: http://www.telcordia.com

United States Department of State, Overseas Security Advisory Council, "Personal Security Guidelines For the American Business Traveler Overseas", Department of State Publication10214, Bureau of Diplomatic Security, Released November 1994.

United States Department of State Travel Warnings and Overseas Security Advisory Council (OSAC): http://www.ds-osac.org/ and http://travel.state.gov/travel_warnings.html

United States Nuclear Regulatory Commission; FY 1991 Organization Factors Research and Applications Progress Report, US Nuclear Regulatory Commission Policy Issues, SECY-92-00, Jan. 1992.

Winsor, D. A.; Communications failures contributing to the challenger accident: An example for technical communicators, IEEE Transactions on Professional Communications, vol. 31, pp. 101-107, 1988.

Wireless Emergency Response Team (WERT) September 11, 2001 Terrorist Attacks on the New York City World Trade Center, October, 2001. www.wert-help.org.

Appendix 3. Acronyms

AMPS – Advanced Mobile Phone Service
ANSI - American National Standards Institute
ATIS – Alliance for Telecommunications Solutions
BITS - Financial Services Roundtable
BITS - Building Integrated Timing System
CBRN - Chemical, Biological, Radiological, Nuclear
CDMA – Code Division Multiple Access
CEV - Controlled Environment Vault
CLEC – Competitive Local Exchange Carrier
CME – Coronal Mass Ejection
COMSOC - IEEE Communications Society
COW - Cell on Wheel
CQR – IEEE Technical Committee on Communications Quality & Reliability
CTIA - Cellular Telecommunications and Internet Association
C-TPAT – Trade Partnership Against Terrorism
EMI – Electro-Magnetic Interference
ERT – Emergency Response Team
ESD – Electro-Static Discharge
FACA – Federal Advisory Committee Act
FEMA – Federal Emergency Management Agency
FCC – Federal Communications Commission
GETS – Government Emergency Telecommunications Service
GSM - Global System for Mobile Communications
HEMP – High Energy Modulated Pulse
HVAC - Heating, Ventilation and Air Conditioning
IEC - International Engineering Consortium
IEEE - Institute of Electrical and Electronics Engineers
IETF - Enternet Engineering Task Force
IP – Internet Protocol
ISAC – Information Sharing and Analysis Center
ITU - International Engineering Consortium
LMR – Land Mobile Radio
MSC – Mobile Switching Center
MTSO – Mobile Telephone Switching Office
NANOG - North American Network Operators' Group
NARUC - National Association of Regulatory and Utility Commissioners
NIST - National Institute of Standards and Technology
NCC – National Coordinating Center for Telecommunications
NCIC – National Crime Information Center
NCS – National Communications System
NERC - North American Electric Reliability Council
NFPA - National Fire Prevention Association
NIPC – National Infrastructure Protection Center
NPSTC - National Public Safety Telecommunications Council
NRC – Network Reliability Council
NRIC – Network Reliability and Interoperability Council
NRSC – Network Reliability Steering Committee

NSIE – Network Security Information Exchange
NSSE - National Special Security Event
NSTAC - National Security Telecommunications Advisory Committee
NS/EP – National Security and Emergency Preparedness
NTIA - National Telecommunications and Information Administration
NRIC – Network Reliability and Interoperability Council
NYC DoITT - New York City Department of Technology and Telecommunications
OPASTCO-Organization for the Promotion and Advancement of Small Telecommunications Companies
OSHA – Occupational Health and Safety Administration
PSPTNS – Packet Switched Public Telecommunications Network Services
RF – Radio Frequency
RFP - Request for Proposal
SIA - Securities Industry Association
SLA - Service Level Agreement
SME – Subject Matter Expert
SMS - Short Messaging System
SOW - Switch on Wheels
TDMA – Time Division Multiple Access
Telecom ISAC – Information Sharing and Analysis Center
TSP - Telecom Service Priority
USTA - United States Telecommunications Association
WPS - Wireless Priority Service

Glossary

Router Filtering Rules: Software designed and implemented to direct network traffic, for either operation or security functions

Appendix 4. NRIC VII Charter

CHARTER of the NETWORK RELIABILITY and INTEROPERABILITY COUNCIL – VII

A. The Committee's Official Designation

The official designation of the advisory committee will be the "Network Reliability and Interoperability Council VII" (hereinafter, the “Council”).

B. The Council's Objectives and Scope of Its Activity

The purpose of the Council is to provide recommendations to the FCC and to the communications industry that, if implemented, shall under all reasonably foreseeable circumstances assure optimal reliability and interoperability of wireless, wireline, satellite, cable, and public data networks.[33] This includes facilitating the reliability, robustness, security, and interoperability of communications networks including emergency communications networks. The scope of this activity also encompasses recommendations that shall ensure the security and sustainability of communications networks throughout the United States; ensure the availability of adequate communications capacity during events or periods of exceptional stress due to natural disaster, terrorist attacks or similar occurrences; and facilitate the rapid restoration of telecommunications services in the event of widespread or major disruptions in the provision of communications services. The Council shall address topics in the following areas:

1. Emergency Communications Networks Including E911

The Council shall report on ways to improve emergency communications networks and related network architectures and facilitate the provision of emergency services through new technologies.[34] This means ensuring that emergency communications networks are reliable, survivable and secure. It also means that emergency communications networks (including E911[35]) can be accessed with currently available technologies as well as with new technologies (e.g., Voice-over-the Internet-Protocol (VoIP), text, pictures, etc., as appropriate).

[33] Public data networks are networks that provide data services for a fee to one or more unaffiliated entities

[34] Dale N. Hatfield concluded in *A Report on the Technical and Operational Issues Impacting the Provision of Wireless Enhanced 911 Services* that the current platform for E911 “has serious limitations in terms of speed, scalability, and adaptability. Additionally . . . these limitations not only burden the development of wireless E911 services, but . . . also constrain our ability to extend E911access to a rapidly growing number of non-traditional devices (e.g., PDAs), systems (e.g., telematics) and networks (e.g., voice networks that employ Voice-over-the Internet-Protocol – VoIP).”

[35] “E911” is an acronym for Enhanced 911 service.

The Council shall address the following topics:

a. Near Term Issues for Emergency/911 Services

The Council shall, by December 16, 2005 provide a report that contains near term emergency communications network Best Practices with supporting documentation.

In addition, the Council shall study specific issues that are identified below. The Council shall coordinate with other forums (e.g., Emergency Services Interconnection Forum (ESIF), National Emergency Numbering Association, etc.) so that each issue can be addressed as efficiently and completely as possible. The Council shall:

- Recommend accuracy requirements for location information particularly for rural, suburban, and urban areas and recommend ways to verify that accuracy requirements are met.[36] Investigate location technologies that could improve accuracy and/or reduce cost.
- Develop recommendations that will lead to a consistent format for information passed to Public Service Answering Points (PSAPs) for Phase 1 and 2 call and location information. This format must resolve any inconsistencies that would otherwise result from using vendor specific formats for transmitting information from Mobile Positioning Centers to PSAPs.
- Develop a consistent, common set of timing thresholds for the database queries and for obtaining location information.
- Specify the information that is to be sent to callers when major E911 network elements fail.
- Enumerate and evaluate the factors that should be considered in deciding whether redundant E911 tandems and alternate PSAPs should be provided to avoid a "fast busy" or a recorded message when one or more non-redundant network elements fail.
- Identify all major traffic concentration points in E911 architectures, such as E911 tandems, Selective Routing Databases (SRDB), Mobile Positioning Centers, and Automatic Location Identification (ALI) databases. The Council shall then define metrics and thresholds that should be used to determine where traffic concentrations are unacceptably high. The Council shall develop Best Practices to reduce traffic concentration wherever it has been determined to be too high. This includes developing Best Practices for the size and diversity of different databases. This may also include developing Best Practices aimed at improving the database process or reducing the number of database queries.

[36] The work of ESIF Study Group G will be considered in this effort.

- Recommend ways to extend E911 services to satellite communications.

- Recommend ways to provide location information to PSAPs for calls originating from multi-line telephone systems (MLTS).

Interim Milestones

By December 17, 2004, the Council shall present a report recommending accuracy requirements for Phase 2 and ways by which compliance with these requirements can be objectively verified.

By April 4, 2005, the Council shall present a report recommending a consistent format for information that is to be passed to PSAPs for Phase 1 and 2 location information; and a consistent set of thresholds for the time required to complete database queries, and the metrics/thresholds for determining unacceptably high traffic concentration points.

By April 4, 2005, the Council shall present a report recommending the ways by which E911 services can be extended to satellite communications. That report shall also specify the information to be sent to the person originating the E911 call when major failures occur in E911 networks.

Final Milestone

By December 16, 2005, the Council shall present a report recommending ways and describing Best Practices to address near-term E911 issues. The report shall include issues from the earlier interim reports as well as recommend ways to extend E911 to MLTS. Finally, the report shall recommend Best Practices addressing high E911 network concentration points.

b. Long Term Issues for Emergency/E911 Services

The Council shall present a report recommending specific architecture properties that emergency communications networks are to provide by the year 2010 along with a generic network architecture that meets those properties. A set of architectures may be recommended depending on the characteristics of the area served. A plan as to how that architecture can be achieved, and how the current architecture can be evolved into the future architecture, shall be provided.

The Council shall:

- Recommend whether the Internet Protocol (IP) technology should be used to improve E911 services and, if so, how it may be used. In this regard, the Council shall address the future dependence of emergency communications networks on IP networks, and in particular, whether IP technologies should be used to get information to and from the PSAPs as communications networks continue to evolve. The potential use of IP to streamline the E911 network shall be addressed.

- Recommend what additional text and data information that emergency communications networks should be capable of receiving. This additional information may include text information (e.g., Instant messaging, e-mail, Short Message Service), pictures (e.g., from cellular phones), paging information, information from concierge services, Intelligent Vehicle Systems, automatic crash notification systems, etc. Recommend generic emergency communications network architecture(s) that will enable PSAPs to receive the recommended information.

- Recommend generic architecture(s) that will allow PSAPs to receive Voice-over-IP (VoIP) E911 calls and their associated call and location information.

- Recommend a long term strategy for processing overflow traffic from PSAPs.

- Recommend ways to modernize and improve the existing methods to access PSAPs (e.g., replacing Centralized Automatic Message Accounting (CAMA) trunks).

- Evaluate the feasibility and advisability of having a National/Regional PSAP to process overflow traffic efficiently from local PSAPs and to provide an interface for national security connectivity. Recommend whether the existing PSAP structure is adequate and whether alternate designs such as regional PSAPs should be explored.

Interim Milestones

By September 25, 2004, the Council shall present a report recommending the properties that network architectures must meet by the year 2010. These shall include the access requirements and service needs for emergency communications in the year 2010.

By June 24, 2005, the Council shall present a report recommending generic network architectures for E911 that can support the transmission of voice, pictures (e.g., from cellular telephones), data, location information, paging information, hazardous material messages, etc. The report shall describe how IP technology should be used.

By September 29, 2005, the Council shall present a report that identifies, in detail, the transition issues for the recommended generic network architectures and how the methods of accessing PSAPs should be modernized.

Final Milestone

By December 16, 2005, the Council shall present a final report describing the properties of the network architectures, the recommended generic network architectures, the transition issues, and the proposed resolutions of these transition issues along with recommended time frames for their implementation. The report shall also present conclusions on the feasibility and advisability of having a National/Regional PSAP and how the existing PSAP structure should be altered.

c. Analysis of Effectiveness of Best Practices Aimed at E911 and Public Safety

The Council shall determine the effectiveness of all Best Practices that have been developed to address E911 and Public Safety. The Council shall also:

- Analyze all outages related to E911 that have been reported pursuant to 47 C.F.R. § 63.100 and determine which Best Practices most clearly apply to E911 outages. The Council shall present recommendations on ways to reduce E911 outages. In addition it shall make recommendations on ways to improve the relevance of the FCC-Reportable Outage data for improving Emergency Communications. This includes defining direct causes and root causes which are better attuned to E911.

- Analyze 63.100 outages related to E911 to identify E911 architecture vulnerabilities.

- Make the language that is contained in the E911 NRC/NRIC Best Practices more precise so that E911 outages will be prevented and the level of compliance with each Best Practice can be reliably measured.

Interim Milestones

By September 25, 2004, the Council shall present a report containing its analysis of 63.100 outages related to 911/E911 and the Best Practices that are most applicable to E911 outages. The report shall also identify E911 architecture vulnerabilities.

By June 24, 2005, the Council shall present a report on its survey to determine how effective Best Practices have been for emergency communications.

Final Milestone

By December 16, 2005, the Council shall submit a report containing the newest version of each of the Best Practices for emergency communications. The report shall be based on its Best Practices survey and shall include revised language for the Best Practices to make them more precise. The report shall also summarize conclusions from its analysis of 63.100 outages.

d. Communication Issues for Emergency Communications Beyond E911

The Council shall present a report defining the long term network requirements for transmitting emergency services information emergency services personnel that is beyond the scope of E911 networks. E911 networks handle transmitting information from those originating E911 calls to PSAPs but not from PSAPs (or from some other network element) to emergency services personnel. The Council shall identify target architectures that will be able to transmit the needed information about the emergency event from PSAPs to emergency services personnel and to aid in coordinating emergency services activities. The Council shall also define the long term communication networks that shall be needed to transmit information from E911 calls to the Department of Homeland Security.

In this regard, the Council shall:

- Recommend whether IP architectures should be used for communications between PSAPs and Emergency Communications systems and personnel and, if so, how it may be used.

- Recommend how methods for accessing Emergency Services Personnel by PSAPs should be modernized.

- Recommend architectures that will allow PSAPs (or other network elements) to send text, pictures and other types of data, such as automatic crash information, to Emergency Services Personnel.

- Recommend the most appropriate role of 911/E911 in major disasters and for terrorist attacks.

Interim Milestones

By December 17, 2004, the Council shall present a report describing the properties that network architectures for communications between PSAPs and emergency services personnel must meet by the year 2010. These recommendations shall include the access requirements and service needs for emergency communications in the year 2010.

By September 29, 2005, the Council shall present a report that recommends the network architectures for communications between PSAPs and emergency service personnel that can support the transmission of voice, pictures (e.g., from a cellular phone), data, location information, paging information, hazardous material messages, etc. The report shall describe whether and how IP technology should be used.

By December 16, 2005, the Council shall present a report describing the transition issues for the recommended target architectures along with its recommended role for 911/E911 in major disasters and terrorist attacks.

Final Milestone

By December 16, 2005, the Council shall present a final report describing the properties of the target architectures for PSAP to emergency services personnel communications, the recommended network architectures, the transition issues, and a proposed resolution of these transition issues along with a time frame for their implementation.

2. Homeland Security Best Practices

By December 16, 2005, the Council shall present a final report that describes, in detail, any additions, deletions, or modifications that should be made to the Homeland Security Best Practices that were adopted by the preceding Council.

3. Best Practices for Wireless and Public Data Network Services

Building on the work of the previous Councils, as appropriate, this Council shall continue to develop Best Practices and refine or modify, as appropriate, Best Practices developed by previous Councils aimed at improving the reliability of wireless networks, wireline networks, and public data networks. In addition, the Council shall address the following topics in detail.

a. Best Practices for the Wireless Industry

The Council shall evaluate the efficacy of all Best Practices that have been developed for the wireless industry. The Council shall perform a gap analysis to determine areas where new wireless Best Practices are needed. The Council shall survey the wireless industry concerning the effectiveness of the Best Practices. The Council shall focus on the special needs of the wireless industry and refine existing Best Practices to focus their applicability to the wireless industry.

Interim Milestones

By December 17, 2004, the Council shall provide a report describing the results of the gap analysis of Best Practices aimed at the reliability of wireless networks.

By April 4, 2005, the Council shall complete its survey of the effectiveness of the Best Practices for the wireless industry.

Final Milestone

By September 29, 2005, the Council shall provide a report recommending the Best Practices for the wireless industry including the new Best Practices that particularly apply uniquely to wireless networks.

b. Best Practices for Public Data Network Services

The Council shall evaluate the applicability of all Best Practices that have been developed for public data network providers. The Council shall perform a gap analysis to determine areas where new Best Practices for these providers are needed. The Council shall survey providers of public data network services, including Internet data services providers, concerning the efficacy of existing Best Practices. The Council shall focus on the special needs of public data services providers and refine existing Best Practices to improve their applicability to Internet data services and other public data network services.

Interim Milestones

By December 8, 2004, the Council shall provide a report describing the results of the gap analysis of Best Practices aimed at the reliability of Internet data services.

By April 29, 2005, the Council shall complete its survey of the effectiveness of the Best Practices for Internet data services.

Final Milestone

By September 25, 2005, the Council shall provide a report recommending the Best Practices for Internet data services providers including the new Best Practices that particularly apply to public data network service providers.

4. Broadband

The Council shall present recommendations to increase the deployment of high-speed residential Internet access service. The Council shall include Best Practices and service features that are, and will be, technology-neutral. The Council's recommendations shall be prepared in such a way as: (1) to ensure service compatibility; (2) to facilitate application innovation; and (3) to improve the security, reliability and interoperability of both residential user systems and service provider systems.

C. Period of Time Necessary for the Council to Carry Out Its Purpose

The Council will have two years to carry out the purposes for which it was created.

D. Official to Whom the Council Reports

The Council shall report to the Chairman of the Federal Communications Commission.

E. Agency Responsible for Providing Necessary Support

The Federal Communications Commission will provide the necessary support for the Council, including the meeting facilities for the committee. Private sector members of the Council shall serve without any government compensation and shall not be entitled to travel expenses or per diem or subsistence allowances.

F. Description of the Duties for Which the Council is Responsible

The duties of the Council will be to gather the data and information necessary to submit studies, reports, and recommendations for assuring optimal communications services within the parameters set forth in Section B above.

G. Estimated Annual Operating Costs in Dollars and Staff Years

Estimated staff years that will be expended by the Council are three (3) for FCC staff and 12 for private sector and other governmental representatives. The Council's estimated operating cost to the FCC is $100,000 per year.

H. Estimated Number and Frequency of Council Meetings

The Council will meet at least three times per year. Informal subcommittees may meet more frequently to facilitate the work of the Council.

I. Council's Termination Date

Original filed on January 6, 1992; December 4, 1998 (amended); December 9, 1999 (renewed); December 26, 2001 (renewed); December 29, 2003 (renewed); April 15, 2004 (amended).

Appendix 5. Attributes of Wireless Networks

Wireless Networks are . . .

- Growing rapidly
- In a Competitive industry
- Data is inherently slow from a portability perspective
- Corporate Data Networks are not fast enough
- Wireless networks have a lot of advertisements
- Advertisements raise Reliability expectations of the End Users
- Are replacing landline networks for voice
- Are leveraged against the wireline network from a transport perspective
- Are isolated without wireline networks
- Similar to wireline except for the access portion of the network
- Secure connections to corporate infrastructure via PDN is cumbersome
- Are subject to very dynamic demand patterns (e.g., WPS)
    - Time of Day, Geographic Area,
- The challenges in dealing with traffic patterns are similar to those of landline
- Networks are engineered for additional capacity
    - Big challenge in knowing how much to over-engineer
- Novel uses of wireless services are creating unusual demand areas (e.g., American Idol)
- Demands and Expectations on the wireless networks are outpacing the quality of the networks
- Environmentally more sensitive than for wireline networks
- More complex configurations than wireline
- Wireless networks have less/fewer standards
- Has issues of RF propagation (reflection, absorption,)
- Emerging trend towards ‘reselling’ (Virtual Network Operators)
- More data applications (push services)
- General public does not understand the limitations of wireless networks
- Networks can be deployed quickly
- Rapid evolution of technology (i.e. every X years)
- Has multiple digital air interface technologies
- Provide facilities-based competition (3-7 providers per market)
- Wireless networks has made location an important issue
- Privacy issues will become an problem
- Fraud susceptibility
- Authentication of user is difficult to track (e.g., adjacent buildings)
- Provide more opportunities for Revenue generation (Feature Rich)
- Commercial Power demands are dynamic
- Property security is difficult (number of cell sites)
- Operations is more difficult (number of cell sites)
- Operations are less structured than wireline
- Consolidation results in multiple operations models/backoffice/customer care/…
- Technology deployment is more complex (software, handsets, roaming)

- SW updates are much more frequent
- Operations people are more versatile (i.e. more network elements, base stations)
- Data applications are expected to grow rapidly (how soon is not clear)
- Data usage is expected to grow as data speeds increase
- E911 is more complex and less reliable than wireline (more possible points of failure, location is difficult)
- More messaging than wireline (i.e., SS7, IP, IS2000)
- Wireless networks are less expensive to deploy
- Soft switches reliable is unknown (new technology, different set of failure modes)
- Reliability model for soft switches is different that wireline switches
- Billing is different, more complex
- Wireless switches are susceptible to outages/overloads due to 3rd party providers services (e.g., voice mail, push applications for data, WIN/wireless IN)
- Are less regulated
- Lawful Intercept (CALEA) for voice/data is more complex
- Network outage recovery may involve multiple devices/elements
- Provisioning from a customer's perspective is faster and with fewer customer dependencies (e.g., Service Provider field support)
- Rapid service deployment creates back office provisioning challenges (pain)
- Wireless' practices and procedures are less mature (but easier to change)
- Wireless networks are very flexible compared to wireline
    - Handsets
    - Air interface
    - Speed of feature deployments
    - Technology evolution
    - Mobility
    - Allows for standards adjustments
    - Easier to deploy additional base stations for special events
- Handset lifecycle is short (1-2 years)
    - Allows upgrades to the handsets via Over-the-Air-Provisioning/Activation (OTPA)
- Cost to consumer is declining due to competition (and lack of regulation)
- Wireless networks don't have the same universal services responsibilities as wireline networks
- More difficult to predict and execute on demand

POWER

- Battery is variable based on cell usage
    - Remote cells last longer
    - Transport Hubs should have generator
    - MTSO all have generators
- Battery life environment impacts battery life (i.e. Temperature)
- Batteries are in a less controlled environment
- Customers are more aware of power outages
- Portable generators are able service more cell sites than fixed generators
- FAA lighting on towers increase the power demand and the criticality of the site
    - Must report within one hour
- Less control of the building environment
- General access to leased facilities is variable

- Less control over the wireless network elements (ability to place generators, ingress/egress, …)
- Wireless carriers are very dependent on LEC capabilities (T1, power survivability)
- Have non-standard generator hook-ups
- Power requirements change more rapidly (i.e. equipment)
- Different power systems are typical (-48v, -24v)
- Carrier hotels require usage of their backup power systems (generators)

ENVIRONMENT

- RF Propagation is based on terrain
  - Technology dependent
  - Seasonality (leaves)
  - Weather (microwave fade)
  - Precipitation
  -
- Wireless elements are more susceptible to temperature variation
- Weather conditions can make some sites inaccessible
- Pests
- Zoning make deployment of cell sites more difficult
- Greater use of disguised sites
- Lightening protection is required at all cell sites
- Greater sharing of facilities between providers (e.g., towers)
  - Municipalities dictating shared towers
  - Increased vulnerabilities
- Mass Calling Events (Hurricanes, storms)

SOFTWARE

- Frequency of SW delivery is vendor dependent
- Software patching in wireless that causes outages is higher than wireline (and wouldn't be tolerated in wireline)
- Wireless software upgrades are not hitless
  - Base stations may not need to be hitless
  - Stable calls should stay up
- Carriers may have carrier specific software
- Carriers have different configurations
  - RF parameters
  - Registrations
- Handset software is difficult to keep up to date
  - PRL updates (Preferred Roaming List)
- Mobility software is complex
  - Handoff
  - Power control
  - Mobility management
  - More network elements
- Greater dependency between transport layer software and core network software

HARDWARE

- Redundancy is accomplished via distributed network and nodes (rather than redundancy within the network element)
- Fault group size are becoming larger
- Hardware footprint is becoming smaller
- More points of failure (i.e. more complex network) and Less Single Point failures

PAYLOAD

- Multiple conversions of payload is typical
- Payload types
    - VOICE
        - EVRC
        - AMR
        - Wireline T1 64k PCM
        - PTT
    - DATA
        - SMS
        - MWI
        - MMS
        - IMS
        - PTT

NETWORK

- Wireless is dependent on wireline core network (similar to wireline) for service offering
    - Voice, SS7, Data, …
- Wireless requires independent synchronization (primary rate source - Stratum 1)
    - Synchronization is not recovered from major networks
    - BITS clock
    - GPS at BSC/cell sites
- Time of Day is required in certain billing applications
- Data Base synchronization specific to roaming is essential
    - Wireless networks lend themselves to validation isolation
        - HLR outages create default service
        - May create problems during an ‘incident’
- Variety of transport (e.g., microwave, Free Space Optics, Wireless line extension)
- Hierarchal networks yield upwardly increasing nodes of concentration
- Characterized by overlays with other competitors networks or own network (i.e. multiple frequencies)
- Multiple equipment suppliers provide nodes in the network
- Varied architectures
    - Proportion of control varies between switch (MSC), intermediate point, or base station
    - Intra-BSC and Intra-BTS switching
- Attributes of wireless network design (not required in wireline)
    - Handoffs (Intra/Inter vendor, technology type, handset implementation)
    - Paging
    - Registration

    - Access Control
    - Power
    - Neighbor list
    - Channel management
    - Frequency planning
- Maintaining quality of services requires maintenance/upkeep of many parameters
- Weird RF Effects (Atmospheric channeling)

HUMAN

- Health concerns related to RF
- Increasing expectations of wireless networks
- Wireless culture is being established at a very young age
- Location identity
- Rapid change in technology is creating training gaps in staff
    - No one with 20 years experience
- Mobile phones carried everywhere by users.
- Used extensively for public safety
- Used for personal safety
- Skill Mismatch (Moving to IP vs. RF)
    - Both for Service Providers and Vendors
- Constant Optimization effort is required

POLICY

- Standards are interpreted and implemented differently
- Some standards are implemented to avoid costs
- Some standards are optional
- FCC plays a major role in spectrum policy
- DHS is rolling out WPS
- Wireless is used for law enforcement
- Not as strongly regulated at the state level as wireline (yet)
- Restricted use of cell phones
- SW/HW is increasingly outsourced.
- Local Jurisdictions play an extensive role in the growth of wireless
    - Adds significant costs
    - Adds unpredictable delays
- Multiple entities with veto power
- Regulators require co-location access
- Major standards difference between US/International
- CFIUS - Role of foreign owned service providers
- DoC/DoJ/DoD (Commerce, Justice, Defense) reviews
- Environmental issues with handset and battery disposal
- Exportation of encryption capabilities on network equipment
- Restriction against use of wireless networks because of security concerns
- PSAPs regulate the sizing of E911 trunk group size (reliability issue)
    - Inconsistency between various E911 regulations

138 items

Appendix 6. Wireless Networks Gaps

1. Business Continuity Planning (4.2.1 Environment)
Existing Best Practices do not address potential impacts of collateral damage from adjacencies.

2. Cell Site Administration (4.2.1 Environment)
Areas of concern include adhering to engineering designs, signage considerations, rogue equipment identification, and avian (i.e. bird) populations.

3. Technical Support and Escalation (4.2.3 Human)
Timely engagement of technical support of the appropriate level during an outage.

4. Offshore Network Operations Control Centers (NOCC) (4.2.3 Human)
Location of NOCC's outside of the US poses some potential risk to the management and security of telecommunication networks.

5. Business Continuity related to Wireless Networks (4.2.4 Network)
There are a number of Best Practices addressing business continuity for communication networks. However, existing NRIC Best Practices do not provide guidance for cell site prioritization and contingency planning for key coverage areas.

6. Air Interface Reliability (4.2.4 Network)
The Network Task group has identified insufficient guidance in existing Best Practices for the unique challenges related to the planning, engineering and optimization of the air interface.

7. Cell Site Administration (4.2.4 Network)
The Network Task group identified the need to gather and maintain cell site information related to the performance, connectivity, and maintenance.

8. Spam Control at Message Centers and MSCs (4.2.5 Payload)
Concerns regarding Spam controls between Message Centers and MSCs need to be addressed.

9. Non-Destructive Fire Suppression (4.2.6 Policy)
Fire suppression systems (e.g. FM200, Halon) as an equivalent alternative to water based sprinklers that could cause damage to equipment thus expanding or prolonging an outage.

10. Emergency Power for Cell Sites (4.2.7 Power)
Emergency power for backhaul (e.g. T1) equipment is needed. Extended backup power for base station equipment is needed.

11. Priority Restoration of Commercial Power to Cell Sites (4.2.7 Power)
Critical cell sites need priority restoration of electrical power

12. Software Controls for Network Overloads (4.2.8 Software)

There are no NRIC Best Practices that provide guidance regarding the software implementation of overload controls so as to effectively manage traffic yet protect the reliability of the most critical nodes in a wireless network.

Appendix 7. Wireless Network Modifications of Existing Best Practices

FG 3A - WIRELESS NETWORK RELIABILITY BEST PRACTICES MODIFIED BEST PRACTICES		
MODIFIED BP NUMBER	RECOMMENDED NEW BP WORDING	REFERENCE / COMMENTS
7-P-1020	Service Providers, Network Operators, and Equipment Suppliers should assess the need for Chemical, Biological, Radiological and Nuclear (CBRN) response program to safely restore or maintain service in the aftermath of fuel/chemical contamination or a Weapons of Mass Destruction (WMD) attack.	
7-P-0517	Equipment Control Mechanisms: Equipment Suppliers should design network elements and associated network management elements with the combined capability to dynamically handle peak load and overload conditions gracefully and queue or shed traffic as necessary (e.g., flow control).	The management of peak load and overload conditions can apply to bearer traffic, signaling traffic, routing and control protocol traffic, network management traffic and messaging, accounting statistics, and flow reporting.
7-P-0555	Equipment Suppliers should continually enhance their software development methodology to ensure effectiveness by employing modern processes of assessment.	Formal design and code inspections may be performed as a part of the software development cycle. Test environments may be enhanced to provide more realistic network settings. Fault tolerance levels and failure probabilities should be shared with Network Operators and Service Providers.
7-P-0559	Service Providers and Network Operators should consider validating upgrades, new procedures and commands in a lab or other test environment that simulates the target network and load prior to the first application in the field.	
7-P-0565	Equipment Suppliers should establish and use metrics to identify key areas and measure progress in improving quality, reliability, and security during product development and field life cycle.	This can be done as follows: request and use customer feedback, jointly perform detailed Root Cause Analysis for reported hardware failures, software faults and procedural errors, working together to establish reliability and performance field objectives. Based on these, suppliers and Network Operators and Service Providers should identify, plan, and implement improvements in the development process as well as processes associated with documentation and training.
7-P-0595	Service Providers and Network Operators should be aware of the dynamic nature of peak traffic periods and should consider scheduling potentially service-affecting procedures (e.g., maintenance, high risk procedures, growth activities) so as to minimize the impact on end-user services.	

FG 3A - WIRELESS NETWORK RELIABILITY BEST PRACTICES

MODIFIED BEST PRACTICES

MODIFIED BP NUMBER	RECOMMENDED NEW BP WORDING	REFERENCE / COMMENTS
7-P-0600	Service Providers and Network Operators should establish and document a process to plan, test, evaluate and implement major change activities onto their network.	
7-P-0447	Service Providers and Network Operators should consider establishing a customer advocacy function to take part in the development and scheduling of changes in order to minimize impact.	See BP 0600
7-P-0603	Schedule System Backups: Network Operators and Service Providers should establish policies and procedures that outline how critical network element databases will be backed up onto a storage medium (e.g., tapes, optical diskettes) on a scheduled basis.	Examples of network databases include router configurations, digital cross connect system databases, switching system images, base station controller images. These policies and procedures should address, at a minimum, the following: Database backup schedule and verification procedures; Storage medium standards; Storage medium labeling; On site and off site storage; Maintenance and certification; Handling and disposal.
7-P-0745	Equipment Suppliers should design equipment so that initializations or upgrades of hardware or software are implemented with minimal or no service impact.	Note: FG3A modicication currently under review by Focus Groups 2A and 3A
7-P-0750	Equipment Suppliers should provide a mechanism for feature activation or deactivation that is not service impacting to end-users (e.g., avoid re-boot, re-start or re-initialization).	
7-P-0448	Equipment Suppliers should, where feasible, provide a memory management capability to reconfigure or expand memory without impacting stable calls or other critical processes (e.g., billing).	
7-P-0805	Service Providers, Network Operators and Equipment Suppliers should work to establish operational standards and practices that support broadband capabilities and interoperability (e.g., video, voice, data, wireless).	Organizations that are working on operational standards and practices supporting broadband services and interoperability: ITU-T, particularly Study Groups 2, Study Group 12 and Study Group 13. Also the IETF, ANSI T1A1, DSL Forum, CableLabs, and the TeleManagement Forum.
7-P-1026	Service Providers and Network Operators should consider creating a corporate policy statement that defines a remote system access strategy, which may include a special process for disaster recovery.	
7-P-1028	Service Providers, Network Operators and Property Managers should engage in preventative maintenance programs for network site support systems including emergency power generators, UPS, DC plant (including batteries), HVAC units, and fire suppression systems.	

FG 3A - WIRELESS NETWORK RELIABILITY BEST PRACTICES

MODIFIED BEST PRACTICES

MODIFIED BP NUMBER	RECOMMENDED NEW BP WORDING	REFERENCE / COMMENTS
7-P-1031	Service Providers and Network Operators should consider entering into Mutual Aid agreements with partners best able to assist them in a disaster situation using the templates provided on the NRIC and NCS websites. These efforts could include provisions to share spectrum, fiber facilities, switching, and/or technician resources.	See http://www.ncs.gov/ncc/nccmaa/nccmaa_toc.html and http://www.nric.org/meetings/meeting20020913.html
7-P-1033	Network Operators should develop a strategy for deployment of emergency mobile assets such as Cell on Wheels (COWs), cellular repeaters, Switch on Wheels (SOWs), transportable satellite terminals, microwave equipment, power generators, HVAC units, etc. for emergency use or service augmentation for planned events (e.g., National Special Security Event (NSSE)).	
7-P-5064	Service Providers, Network Operators and Property Managers should alarm and monitor critical electronic equipment areas to detect parameters that are outside operating specifications (e.g., temperature, humidity).	
7-P-5072	Service Providers, Network Operators and Equipment Suppliers should perform risk assessments on key network facilities and control areas on a regular basis. Assessments should address natural disasters and unintentional or intentional acts of people on facility or nearby structures.	
7-P-5089	Service Providers, Network Operators and Equipment Suppliers should establish, implement and enforce appropriate procedures for the storage and movement of equipment and material, including trash, around facilities and campuses.	This will help minimize potential theft, tampering, introduction of harmful materials, inadvertent exposure of critical information, and reduce the risk of fire. Note: FG3A modicication currently under review by Focus Groups 2A and 3A
7-P-5139	Service Providers, Network Operators and Equipment Suppliers should consider establishing procedures for managing personnel who perform functions at disaster area sites.	
7-P-5145	Network Operators should establish plans to perform interference analysis and mitigation to ensure timely resolution of all cases of interference (e.g., caused by equipment failure, intentional act/sabotage or frequency overlap). Where feasible, analysis should enable identification of type and general location of interference source.	

Appendix 8. Wireless Network New Best Practices

FG 3A WIRELESS NETWORKS		
NEW BP #	NEW BP WORDING	COMMENTS
7-P-0499	Network Operators and Service Providers should, where feasible, deploy SPAM controls in relevant nodes (e.g., message centers, email gateways) in order to protect critical network elements and services.	
7-P-0450	Property Managers should maintain current documentation that ensures that the tower loading is consistent with the engineering design (e.g., antenna loading, feedline loading, ice or wind loading).	
7-P-0451	Service Providers, Network Operators and Property Managers should conduct a periodic physical site audit to update and maintain accurate antenna and tower engineering documentation in order to positively identify every item on the tower structure (e.g., identifying rogue antennas).	
7-P-0452	Service Providers, Network Operators and Property Managers should post emergency contact number(s) and unique site identification in an externally visible location at unmanned communication facilities (e.g., towers, cell sites, Controlled Environment Vault (CEV), satellite earth stations). This signage should not reveal additional information about the facility, except when necessary.	Examples of site identification may include: Latitude/Longitude, Real Estate ID, FAA number, FCC registration number, ASR (Antenna Structure Registration) data base, cell ID, address, location. See Best Practice 5120.
7-P-0453	Service Providers and Network Operators should prepare for HVAC or cabinet fan failures by ensuring that conventional fans are available to cool heat-sensitive equipment, as appropriate.	
7-P-0454	Network Operators and Service Providers should consider establishing technical and managerial escalation policies and procedures based on the service impact, restoration progress and duration of the issue.	
7-P-0455	Equipment Suppliers should consider a program to remove cards or modules from circulation that have a history of failure even if tests indicate "No Trouble Found".	
7-P-0456	Network Operators should maintain records of pertinent information related to a cell site for its prioritization in disaster recovery and key coverage areas (e.g., emergency services, government agencies, proximity to hospitals).	

FG 3A WIRELESS NETWORKS		
NEW BP #	NEW BP WORDING	COMMENTS
7-P-0457	Network Operator and Service Provider should develop a process to identify RF dead spots and, where feasible, provide a solution to fill the dead spot with RF coverage.	
7-P-0458	Network Operator should verify when a new cell site is added to the network that calls handoff between cells.	
7-P-0459	Equipment Suppliers should design outdoor equipment (e.g., base station) to operate in expected environmental conditions (e.g., weather, earthquakes).	
7-P-0460	Network Operators should ensure that equipment is installed in accordance with equipment suppliers' stated environmental specifications.	
7-P-0461	Equipment Suppliers should provide the capability to test failover routines of redundant network elements.	
7-P-0462	Network Operators should work in conjunction with local municipalities to anticipate RF capacity needs driven by changes in vehicle traffic patterns or other demographics.	
7-P-0463	Network Operators and Service Providers should consider establishing agreements so that mobile customers can roam on other providers' networks.	
7-P-0464	Network Operators and local municipalities should cooperate on zoning issues that affect reliability of communication networks serving the public good (e.g., noise from emergency backup power generators, aesthetics of tower placement, public safety and health concerns).	
7-P-0465	Network Operators should, during the initial design and periodic reviews of cell site coverage, account for the effects of environmental changes (e.g., new buildings, tree growth, construction materials) that result in attenuation, shadowing, and multipath.	
7-P-0466	Network Operators should, when planning network coverage, take into account link budget impacts due to propagation differences between various spectrum (e.g., 850 MHz vs. 1800/1900 MHz).	
7-P-0467	Network Operators should give consideration to the degree of balance between RF channels on uplinks and downlinks, for both control and traffic.	

FG 3A WIRELESS NETWORKS		
NEW BP #	NEW BP WORDING	COMMENTS
7-P-0468	Network Operators and Property Managers should consider agreements to share in-building antenna infrastructure between multiple service providers in order to make it more feasible to deploy in-building systems.	
7-P-0469	Network Operators and Property Managers should consider the use of cable support (e.g., H-Frames, Ice Bridges) in tower and shelter designs.	
7-P-0470	Network Operators and Property Managers should consider tower and antenna designs that do not attract bird and animal nesting (e.g., no platforms, flush mounted panels, smooth radome).	
7-P-0471	Network Operators and Property Managers should consider remote, electronic antenna aiming and utilize tower-mounted equipment that minimizes the need for tower top maintenance where conditions prevent climbs (e.g., osprey nest, weather conditions).	
7-P-0472	Network Operators and Equipment Suppliers should consider connector choices and color coding to prevent inappropriate combinations of RF cables.	
7-P-0473	Property Managers should consider maintaining a list of authorized climbers and a log of authorized tower climbs.	
7-P-0474	Network Operators and Property Managers should periodically perform grounds maintenance at cell site facilities (e.g., pest control, mow grass, fence maintenance, snow removal).	
7-P-0475	Network Operators and Property Managers should have agreements in place to ensure necessary and timely access to cell sites.	
7-P-0476	Network Operators and Property Managers should consider conducting physical site audits after a major event (e.g., weather, earthquake, auto wreck) to ensure the physical integrity and orientation of hardware has not been compromised.	
7-P-0477	Network Operators, when designing cell sites with high voltage FAA beacons, should consider the potential of electromagnetic coupling into the receivers and, if present, take appropriate steps to mitigate the interference (e.g., squelch, physical separation, shielding).	
7-P-0478	Network Operators, when designing cell sites, should allow for deviation in elevation angle and azimuth resulting from deflection of the supporting structure (e.g., sun, load distribution, wind).	

FG 3A WIRELESS NETWORKS		
NEW BP #	NEW BP WORDING	COMMENTS
7-P-0479	Network Operators should take into consideration fundamental technology differences when operating multiple RF technologies in an existing system. Radio Frequency Interference (RFI) sources (e.g., intermodulation, out of band emissions, receiver overload), link budgets, and performance metrics (e.g., data rates, latency, capacity) should be evaluated.	
7-P-0480	Network Operators and Property Managers should periodically inspect antennas, waveguide, and ancillary hardware to insure physical integrity and the absence of physical movement which can create intermittent and localized intermodulation interference generators (e.g., rusty joints) and/or alter predicted antenna radiation patterns (e.g., antennas swinging around in the wind) potentially creating interference.	
7-P-0481	Network Operators and Property Managers should ensure appropriate spacing between all antennas at a cell site in order to avoid interference, intermodulation, or other detrimental effects.	
7-P-0482	Network Operators should utilize RF propagation and other modeling tools to analyze and optimize designs to avoid interference and improve network performance.	
7-P-0483	Network Operators should have a master cell site database with configuration parameters, connectivity, and performance statistics that can be used to analyze and audit cell site performance.	
7-P-0484	Network Operators should have a program (e.g., automated drive test equipment, network probes) to monitor and detect network performance anomalies.	
7-P-0485	Network Operators should optimize cell sites, including relationships between neighboring cells, using a combination of drive testing and network statistics.	
7-P-0486	Network Operators should have an ongoing RF performance improvement process to reduce blocks, drops, and access failures.	
7-P-0487	Network Operators should have procedures in place to identify and correct degradations in cell site performance resulting from defects in feedlines and antennas (e.g., moisture, bullets, kinking).	

FG 3A WIRELESS NETWORKS		
NEW BP #	NEW BP WORDING	COMMENTS
7-P-0488	Network Operators and Service Providers should ensure that critical wireless circuits (e.g., high priority cells, SS7 circuits, 911 circuits) are registered with Telecom Service Priority (TSP).	Also, see BP 0587
7-P-0489	Network Operators, Service Providers and Equipment Suppliers should consider provisions in labor contracts to provide for cooperation between union and non-union personnel during disaster recovery situations.	Also, see BP 1024
7-P-0490	Network Operators and Service Providers should consult National Fire Prevention Association Standards (e.g., NFPA 75 and 76) for guidance in the design of fire suppression systems. When zoning regulations require sprinkler systems, an exemption should be sought for the use of non-distructive systems.	Communications equipment can be easily damaged by water from sprinkler systems.
7-P-0491	Service Providers, Network Operators and Equipment Suppliers should, where programs exist, coordinate with local, state and/or federal emergency management and law enforcement agencies for pre-credentialing to help facilitate access by technicians to restricted areas during an event.	
7-P-0492	Network Operators should provide back-up power (e.g., some combination of batteries, generator, fuel cells) at cell sites and remote equipment locations, consistent with the site specific constraints, criticality of the site, the expected load and reliability of primary power.	
7-P-0493	Network Operators and Property Managers should consider placing fixed power generators at cell sites, where feasible.	
7-P-0494	Network Operators and Property Managers should consider including a provision in cell-site contracts for back-up power.	
7-P-0495	Network Operators and Property Managers should consider pre-arranging contact information and access to restoral information with local power companies.	
7-P-0496	Network Operators and Property Managers should consider storing their portable generators at critical sites that are not otherwise equipped with stationary generators.	
7-P-0497	Network Operators and Property Managers should consider connecting the power load to portable generators where they are stored, and configuring them for auto-engage in the event of a failover.	

Appendix 9. Acknowledgements

The Focus Group leaders recognize the following:

Participating Companies
The organizations that send technical experts are recognized for their vital support. Without the commitment of such companies to the reliability of the nation's wireless networks, this work could not have been completed.

Task Group Leaders
The development of industry consensus required significant leadership and attention to a wide variety of concerns and interests. The Task Group leaders provided much of this talent and energy.

Task Group Members
The technical contributions and diligence in participating in industry consensus development is highly commendable. In many instances, members used significant personal time to support the completion of the team's mission.

Other Experts
Countless other subject matter experts were engaged from within and from without the participating companies. Their insights provided additional strength to the Task Group's competence.