NRIC VII
Network Reliability and Interoperability Council VII

Issue 1 –

December 2004

FOCUS GROUP 3A

Wireless Network Reliability

Gap Analysis Report

About this Document

Per the Council Charter, the Wireless Focus Group plans three issues of its report as follows, with each issue making vital information available to the communications industry as it became available.

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

- Issue 2, Effectiveness Report. This second Issue will include a survey of the effectiveness of the Best Practices for the wireless industry.

- Issue 3, Final Report. The third Issue will include additional Best Practices for the wireless industry.

Subsequent versions integrate the newer material with that of the previous issue, and thus make the earlier issues obsolete.

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 first report and first deliverable of the Wireless Network Reliability Focus Group. 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.

The Wireless Network Reliability Focus Group reports 5 major accomplishments in this first issue:

1. engagement of over 50 industry subject matter experts (Section 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
5. identification of 12 gaps in existing NRIC Best Practices

1.1 *Major Findings*

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

TABLE 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 *Summary of Conclusions and Recommendations*

The Focus Group is already underway with industry consensus discussions directed toward developing voluntary Best Practices that address these identified gaps in existing NRIC Best Practices. Some gaps may be forwarded to other Focus Groups, and still others, if no best practice exists, may remain as an area for attention for the industry.

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.

Issue 2 of this report will report on the effectiveness of NRIC network reliability Best Practices for Wireless Networks.

Issue 3 of this report will identify existing Best Practices and recommend new Best Practices for Wireless Networks.

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. (scope to be defined)” 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 10). The Mission is almost verbatim from applicable sections of the Council Charter, with a few exceptions for clarification.

<u>Focus Group 3A Mission</u>

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 will focus 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), 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 and Equipment Suppliers of the public communications infrastructure. The following is a brief definition of the principal organizational components referred to throughout the NRIC Best Practices:[2]

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.

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

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 industry experience regarding 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 introduce a new focus on Emergency Communications Networks. [Figure 1. NRIC VII Focus Group Structure].

Focus Group Structure

Focus Group 1 – Emergency Communications Networks

A - **Near Term Issues**
Chair: Darold Whitmer (Intrado)

B - **Long Term Issues**
Chair: Jim Nixon (T-Mobile)

C – **Network Outages and Best Practices**
Co-Chair: Nancy Pollock (Minnesota Metro 911 Board)
Co-Chair: Bob Oenning (State of Washington)

D – **PSAP / Emergency Communications beyond 911**
Chair: RoxAnn Brown (Metropolitan Government of Nashville & Davidson County)

Focus Group 2 – Homeland Security

A – **Infrastructure**
Chair: John Stogoski (Sprint)

B - **Cyber Security**
Chair: Bill Hancock (Savvis)

Focus Group 3 - Network Reliability

A - **Wireless Network Reliability**
Co-Chair: John Quigley (Sprint)
Co-Chair: Karl Rauscher (Bell Labs, Lucent Technologies)

B - **Public Data Network Reliability**
Co-Chair: David Frigeri (Internap Network Services)
Co-Chair: Karl Rauscher (Bell Labs, Lucent Technologies)

Focus Group 4 – Broadband
Chair: Mary Retka (Qwest)

Figure 1. NRIC VII Focus Group Structure

2.3.1 Attributes of Wireless Networks

Previous Councils have increasingly included both the subject matter of wireless and the related expertise. For example, the Fifth Council included a Subcommittee that reviewed all existing Best Practices to determine applicability to wireless networks and services. A Wireless network key word was used to identify applicable Best Practices; some required minor refinements of modifications.[3] The Sixth Council also included both a focus and 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

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

Councils, the FCC Designated Federal Officer 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 need 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 8 Task Groups. The 8 areas associated with these tack Groups provided comprehensive, systematic coverage of communications infrastructure (Figure 4).

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]

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

[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.

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 being 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. An industry survey is planned for 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
- 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 2.1.1) specifies 12 specific actions that are to be undertaken by the Focus Group.

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

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 for a, government, others). Figure 2 lists the participating organizations and their representatives. In addition to the Focus Group members, additional experts were engaged with these organizations and from other organizations to support the vulnerability assessment 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	**Nextel**	David Proffer
AT&T	Victor DeVito*	**Nokia**	Slawomir Deja Mauizio Gallucci
Cingular	Ray Fannon Rich Moczygemba	**Qwest Wireless**	Sherman W. Phillips
Comcast Cable	Dean Brewster	**SBC**	John Chapa
Cox Communications	Mark Adams	**Sprint**	Bill Hitchcock* Brad McManus*
Dobson	Scott Jones	**Verizon Wireless**	Chris Oberg
Intelsat	Mark Neibert	**T-Mobile**	Tom Ellefson John Mardula*
MCI	Mike Sheffield		

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
Harris Corporation	Steven Warwick		

OTHERS

ATIS	Bill Klein (A)	**NCS**	Perry Fergus
CTIA	Rick Kemper	**NYC DOITT**	Mitchel Ahlbaum
FCC	Jeff Goldthorp (A) Kent Nilsson (A)	**SAIC**	Hank Kluepfel (A)
		SpectraSite	Ted Abrams

Figure 2. 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 to take 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

Using the eight dimensions of the Communications Infrastructure identified in the following Figure 3, the Focus Group formed Task Groups. The Wireless Network attributes, issues and problems, and priority topics were distributed across these Task Groups, as appropriate.

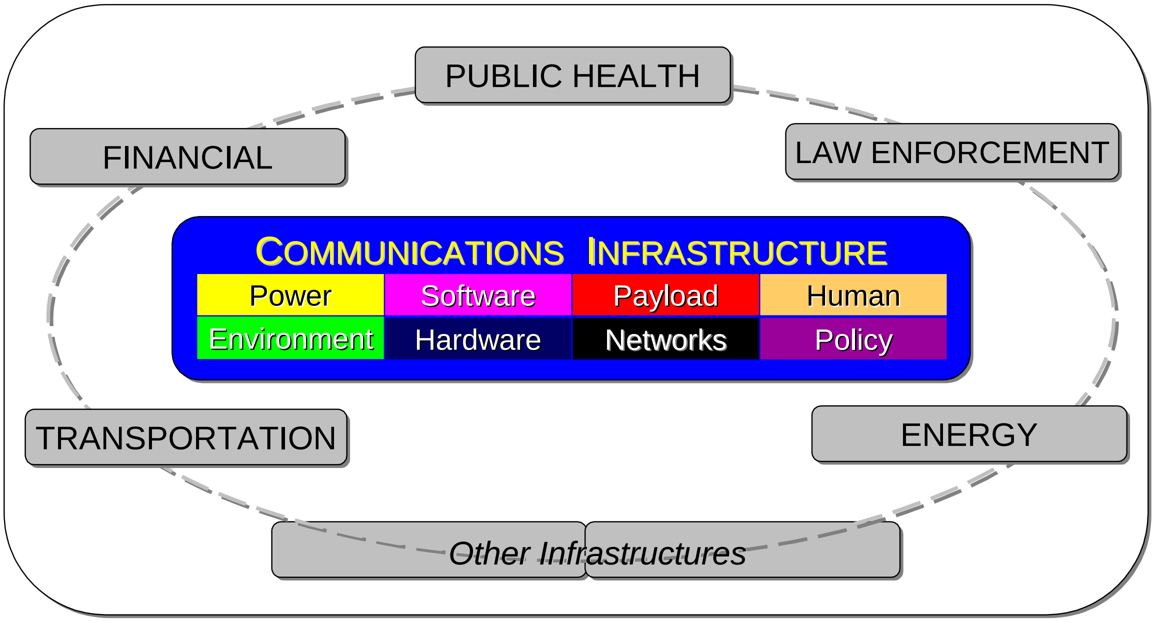

Figure 3. Communications Infrastructure

The Task Group and Leaders are as follows:

- Environment Task Group – Victor DeVito, AT&T
- Hardware Task Group – 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
- 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 meeting scheduled from May 2004 through November 2004 are shown in Table 2:

Table 2. Meeting Statistics

Meeting Type	Participant-Hours
Conference Call	~250
Workshops	~1275
Total	**~1525**

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 days.

Table 3. Meeting Summary

MEETING NUMBER	DATE	MEETING TYPE	PARTICIPANTS
1	May 7, 20024	Conference Call	14
2	May 21, 2004	Workshop (DC)	15
3	May 28, 2004	Conference Call	18
4	June 8, 2004	Workshop (DC)	22
	June 9, 2004	Workshop (DC)	17
5	June 28, 2004	Conference Call	19
6	July 13, 2004	Workshop (KC)	17
	July 14, 2004	Workshop (KC)	18
7	July 29, 2004	Conference Call	19
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
10	October 13, 2004	Workshop (NV)	19
	October 14, 2004	Workshop (NV)	16
11	November 1, 2004	Conference Call	18
12	November 10, 2004	Workshop (DC)	12
	November 11, 2004	Workshop (DC)	14
13	November 12, 2004	Conference Call	10
14	November 15, 2004	Conference Call	9

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)
- 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)
- Organization for the Promotion and Advancement of Small Telecommunications Companies (OPATSCO)
- President's National Security Technical Advisory Council (NSTAC)
- 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)

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

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.

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.

3 Background

3.1 Gap Analysis

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

TABLE 4. 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

3.2.1 ENVIRONMENT

3.2.1.1 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; 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 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.

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

- ❑ 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 4 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. Table 5 lists the Environment Task Group participants

Table 5. Environment Task Group Participants

Name	Company	Sub-team Leader
Victor DeVito	AT&T, ***Leader***	Environmental Task Group Leader
Julie Briggs	AT&T	
Ralph Collipi	AT&T	HAZ Mat (Co-lead)
Linda Ferro	AT&T	HAZ Mat (Co-lead) Business Continuity
Eric Hounchell	BatteryCorp	
Miles Schreiner	T-Mobile	Equipment
John Chapa	SBC	Buildings
Jim Runyon	Lucent Technologies	
Ted Abrams	Spectra Site	Tower Sites & Landscaping
Leo Palumbo	AT&T	

3.2.1.3 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 Environment 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 environment factors that can impact network reliability and the existing 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 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. 51 Best Practices identified through the areas of expertise were found to have potential application to the reliability of wireless networks[9] and satisfactorily addressed to varying degrees the particular environmental issue or item initially identified by the FG 3A team.

The Task Group's gap analysis determined that while the majority of the identified issues and items generated by the FG 3A Team had existing Best Practices to mitigate the threat posed by that particular issue or item, there were gaps to the issues/items list 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 by existing best practices and required further review.

The task group has identified the following 2 Gaps:

1. Business Continuity Planning
Existing Best Practices do not address potential impacts of collateral damage from adjacencies In addition, access to remote elements (e.g. cell sites), for restoration of service, is often delayed due to security concerns (e.g. pre-credentialing).

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

From the team's further analysis of these outstanding gap issues and items not fully mitigated by existing practices, additional new or edited Best Practices were researched and recommended back to the Focus Group for additional discussion.[10]

3.2.2 HARDWARE

3.2.2.1 Subject Matter

Hardware has a fundamentally-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,

[9] An NRIC Best Practices web site search for the various areas of expertise under study revealed the following 51 Best Practices as applicable to the environmental issues and items: 6-6-5072, 6-6-5073, 6-6-1004, 6-6-0599, 6-6-5207, 6-6-1067, 6-6-0655, 6-6-0698, 6-5-0699, 6-6-5204, 6-6-5214, 6-6-5232, 6-5-0544, 6-5-0598, 6-6-5275, 6-6-1030, 6-5-0597, 6-5-0588, 6-6-1001, 6-6-0577, 6-6-8068, 6-6-5259, 6-6-1020, 6-6-5178, 6-6-1051, 6-6-5138, 6-6-5139, 6-6-1020, 6-6-5224, 6-6-5230, 6-6-5064, 6-6-5119, 6-5-0699, 6-6-5006, 6-6-5008, 6-6-5021, 6-6-5011, 6-6-5012, 6-6-5026, 6-6-0723, 6-5-0651, 6-5-0652, 6-6-5120, 6-6-5149, 6-6-5148, 6-5-0647, 6-5-0652, 6-6-5229, 6-6-5197, 6-6-0636, 6-6-5056

[10] The Task Group recognized that there were a number of issues/items that were more appropriate to be addressed by the Hardware, Power, and Policy teams. With agreement from the Task Group leaders, these items were assigned to the new Task Groups for review and recommendation. In addition, the Task Group recognized items 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.

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 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 6 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 6. Hardware Task Group Participants

Name	Organization
Robin Roberts	Cisco Systems
Rick Krock	Lucent Technologies
Lester Buczek, ***Leader***	Motorola
John Bassett	Motorola

3.2.2.3 Gap Analysis

The Council Charter directs the Focus Group to "*perform a gap analysis to determine areas where new Best Practices for [Public Wireless Networks] 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 public wireless networks.[12] In addition, the Task Group reviewed the

[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)

[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.

work of the previous Council in which the vulnerabilities of Hardware were systematically reviewed.[13]

The task group identified no Gaps:

The Task Group's gap analysis determined that while 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.

3.2.3 HUMAN

3.2.3.1 Human

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 (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 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 4 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 3A Focus Group to review concerns against existing Best Practices from previous NRIC focus groups. Table 7 lists the Human Task Group participants.

Table 7. Human Task Group Participants

Name	Organizatio
John Quigley, ***Leader***	Sprint
David Proffer	Nextel
Dr. Anil Macwan	Lucent Technologies
Rick Krock	Lucent Technologies

3.2.3.3 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

[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.

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 2 Gaps:

1. Technical Support and Escalation

Timely engagement of technical support of the appropriate level during an outage.

2. Offshore Network Operations Control Centers (NOCC)

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

3.2.4 NETWORK

3.2.4.1 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.

[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

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 monitoring, maintaining, 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 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 8 lists the Network Task Group participants.

Table 8. 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 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 is now undergoing detailed analysis to determine the proper disposition. The following dispositions and current status exists 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 has identified the following 3 gaps:

1. 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.

2. 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.

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

Work continues in this area to define Best Practices. The initial list will be exhausted with applicable Best Practices developed, as appropriate. Further brainstorming, analysis and industry research will continue to bring new ideas forward. Existing Best Practices[1] will continue to be reviewed and gap analysis will be performed.

[1] NRIC Best Practices web site keyword search touching the network area resulted in the following: Reliability: 261 Network Operations: 151 Network Design: 73 Network Provisioning: 56

3.2.5 PAYLOAD

3.2.5.1 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 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 public data 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 9 lists the Payload Task Group participants. The team had sufficient expertise to complete this activity.

Table 9. 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 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 Payload 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.[15] In addition, the Task Group reviewed the work of the previous Council in which the vulnerabilities of payload were systematically reviewed.[16] [17]

Several minor refinements have been proposed for the existing Best Practices. These are under consideration and may yield further discussion in a future issue of this report.

The Task Group has identified one Gap:

1. SPAM Control at Message Centers and MSCs

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

[15] 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.

[16] 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.

[17] 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.

3.2.6 POLICY

3.2.6.1 Subject Matter

Policy, as utilized in the 8 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 agreement, 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 10 lists the Policy Task Group participants. The team had sufficient expertise to complete this activity.

Table 10. 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 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 for Policy 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 other 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:

1. 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.

In addition to the aforementioned gap, the group will be proposing several minor modifications to existing practices to ensure their scope includes the needs of the wireless sector.

3.2.7 POWER

3.2.7.1 Subject Matter

The Power Area includes the internal power systems, batteries, grounding, high voltage and other cabling, fuses, back-up emergency generators and fuel.[18] Power is often overlooked as a critical basic element of the communications infrastructure. Without power, networks will not function. In addition, any power problem has the potential to become a catastrophe, potentially damaging other equipment and personnel. The power infrastructure also has the potential for being turned into a weapon to be used to harm the network and network personnel.[19] With over 174,000 cell sites[20], the wireless network presents a number of unique challenges in terms of zoning and building restrictions that impact the ability to provide and maintain power.

3.2.7.2 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 6 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 11 lists the Power Task Group participants. The team had the requisite expertise to complete this activity.

Table 11. Power Group Task Group Participants

Name	Organization
William Hitchcock	Sprint
Richard Krock	Lucent - Bell Labs
John Mardula, ***Leader***	T-Mobile
Leo Palumbo	A&TT
Jim Runyon	Bell Labs, Lucent Technologies
Howard Washer	BatteryCorp

3.2.7.3 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 for Power 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

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

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

[20] CTIA Semi-Annual Wireless Survey, June 2004

specifically to electrical power in wireless networks. To understand the latter boundary, the existing Best Practices pertaining to power (approximately 100[21]) 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.

The Task Group has identified the following 2 gaps:

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

2. Priority Restoration of Commercial Power to Cell Sites.
Critical cell sites need priority restoration of electrical power

These gaps are being addressed by revising existing Best Practices or documenting new Best Practices. These issues are under consideration and will yield further discussion in a future issue of this report.

Events during the past few years (e.g., 2003 Northeast 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 special conference dealing with Emergency Power for remote installations has been organized with broad industry support[22]. In addition, the NRSC is conducting a special study related to the lessons learned from the 4 major hurricanes in 2004. The Power Task Group will consider the findings of these activities as they continue their analysis of power issues.

[21] 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

[22] Technically sponsored by the IEEE CQR

3.2.8 SOFTWARE

3.2.8.1 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 and be stored in 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 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 12 lists the Software Task Group participants:

Table 12. Software Task Group Participants:

NAME	ORGANIZATION
Bentley Alexander, ***Leader***	Ericsson
Srinivasa Anam	Nortel
Slawek Deja	Nokia
Rick Krock	Lucent Technologies
Brad McManus	Sprint
Vijay Patel	T-Mobile
Sherman Phillips	Qwest

3.2.8.3 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 for Software was similar to the process used in other areas as described in Section 2.3.5. Therefore, a gap is herein determined by reviewing known problems with the subject area of “software” that can impact network reliability. Those known problems were then assessed against documented Best Practices involving Software. During the review process, a list of 22 known issues involving software was created. A review of the documented Best Practices revealed 63 practices pertaining to software and the relevance to network reliability.[23]

[23] 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-

In reviewing the known issues, there were five primary categories that the issues were sorted into:

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

The Task Group's gap analysis determined that most issues were addressed by previously documented Best Practices or can be addressed with a slight revision to an existing Best Practice. In a few instances, a new Best Practice or Recommendation may be proposed based on an existing practice addressing a similar, yet distinct subject or discipline. In those few instances where revisions or additions to the existing Best Practices are suggested, they will be presented to the Focus Group and brought forward as a recommendation in a subsequent report.

The Task Group has identified the following gap:

1. 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.

Finally, 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.

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

3.3 Survey of Effectiveness

This section is reserved for Issue 2 of this document.

3.4 Best Practices

This section is reserved for Issue 3 of this document.

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 it its reports that most outages monitored at the national level could have been prevented if existing NRIC Best Practices had been implemented[24]. 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[25]

A survey that focuses on Best Practice effectiveness is planned for 2005.

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.

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 appropriate application of these Best Practices can only be done by individuals with

[24] 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

[25] 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.

sufficient competence to understand them. Although the Best Practices are written to be easily understood, their meaning is often *not* apparent to those lacking experience and/or expertise in the specific job functions related to the practice. 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 year 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.' "[26]**

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

[26] 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 (e.g. 7 in 2004-2005)
Y = the Council in which the Best Practice was last edited (i.e. 6 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

This is the first report and first deliverable of the Wireless Network Reliability Focus Group. 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.

The Wireless Network Reliability Focus Group reports 5 major accomplishments in this first issue:

1. engagement of over 50 industry subject matter experts
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
5. identification of 12 gaps in existing NRIC Best Practices

The 12 gaps are listed in Appendix 6.

The Focus Group is already underway with industry consensus discussions directed toward developing voluntary Best Practices that address these identified gaps in existing NRIC Best Practices. Some gaps may be forwarded to other Focus Groups, and still others, if no Best Practice exists, may remain as an area for attention for the industry.

Issue 2 of this report will report on the effectiveness of NRIC network reliability Best Practices for the wireless industry. Issue 3 of this report will identify existing Best Practices and recommend new Best Practices for the wireless industry.

Appendix 7, *Acknowledgements*, recognizes key contributors to the work of this team.

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.

Appendix 1 - List of Interviewees

To be added in FG 3A Document “Wireless Network Reliability,” Issue 2.

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
CDMA – Code Division Multiple Access
CLEC – Competitive Local Exchange Carrier
CME – Coronal Mass Ejection
COMSOC - IEEE Communications Society
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
IEC - International Engineering Consortium
IEEE - Institute of Electrical and Electronics Engineers
IP – Internet Protocol
ISAC – Information Sharing and Analysis Center
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
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
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
OPATSCO-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
SLA - Service Level Agreement
SME – Subject Matter Expert
TDMA – Time Division Multiple Access
Telecom ISAC – Information Sharing and Analysis Center
USTA - United States Telecommunications Association

Glossary

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

Appendix 4 - 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.[27] 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.[28] This means ensuring that emergency communications networks are reliable, survivable and secure. It also means that emergency communications networks (including E911[29]) 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).

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

[28] 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).”

[29] “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.[30] 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.

[30] 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, absorbtion,)
- 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
  - <u>VOICE</u>
    - EVRC
    - AMR
    - Wireline T1 64k PCM
    - PTT
  - <u>DATA</u>
    - 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 - Gaps

1. **Business Continuity Planning** (4.2.1 Environment)
Existing Best Practices do not address potential impacts of collateral damage from adjacencies In addition, access to remote elements (e.g. cell sites), for restoration of service, is often delayed due to security concerns (e.g. pre-credentialing).

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 - 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.