NRIC VII

Network Reliability and Interoperability Council VII

Issue 1 –

December 2004

# FOCUS GROUP 3B

# Public Data Network Reliability

# Gap Analysis Report

## About this Document

Per the NRIC VII Council Charter, the Public Data Network Reliability 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 Internet data networks.

- Issue 2, Effectiveness Report. This second Issue will include a survey of the effectiveness of the Best Practices for Internet data services

- Issue 3, Final Report. The third Issue will report recommending Best Practices for Internet data services providers including the new Best Practices that particularly apply to public data network service providers.[1]

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

[1] See footnote in Section 2.1.2, *Deliverables*, for additional information on this final deliverable.

# 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 Public Data 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 Public Data Networks.

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

1. Engagement of over 60 industry subject matter experts (Section 2 and 3)
2. Articulation of over 70 attributes of Public Data Networks
3. Consideration of over 200 concerns regarding Public Data Networks
4. Formation of 8 Task Groups that provide systematic coverage of communications infrastructure elements (Section 3)
5. Identification of 11 gaps in existing NRIC Best Practices (Section 3)

## 1.1 Major Findings

The 11 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 | 1 | 3.2.1 |
| Hardware | 0 | 3.2.2 |
| Human | 0 | 3.2.3 |
| Network | 4 | 3.2.4 |
| Payload | 0 | 3.2.5 |
| Policy | 0 | 3.2.6 |
| Power | 2 | 3.2.7 |
| Software | 4 | 3.2.8 |

Examples of identified gaps include:

**Environment**

The Environment Task Group identified one gap in existing, documented NRIC Best Practices related to the complexity of managing growth in third party and multi-tenant environments (e.g., space, power, cooling).

**Network**

The Network Task Group has identified opportunities to enhance NRIC Best Practices in the following areas: the treatment of private address space, routing practice, and design audit.

**Software**

The Software Task Group has identified opportunities to enhance NRIC Best Practices in the area of crash diagnostic memory storage and the use non-volatile memory. There

is added opportunity to improve storage of core dumps and system states associated with a crash.

## 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 Public Data Networks. Issue 3 of this report will identify existing Best Practices and recommend new Best Practices for Internet data services providers.

# 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 public data networks." Specifically, the Charter stated, "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."

### 2.1.1 Mission

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

**Focus Group 3B Mission**

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

**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.**

### 2.1.2 Deliverables

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

**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.[2]**

## *2.2 Scope*

### 2.2.1 Scope Statement

In NRIC VII Focus Group 3B, a Public Data Network (PDN) is defined as a network established and operated for the specific purpose of providing data transmission services for the public. Such networks are considered 'in scope' for Focus Group 3B.

The NRIC VII Focus Group 3B on Public Data Networks Best Practices has classified our scope of coverage into three categories:

1. In Scope for Focus Group 3B:

    - guidance covering the configuration and operation of in-scope networks including general design characteristics, equipment, emergency use of network resources (but not E911), customer interfaces, the impact of government policy recommendations, and any general areas, such as power and security) on which in-scope networks depend.

    - guidance covering inter-provider information and configuration including inter-provider routing configurations, ATM and frame relay NNI, NOC-to-NOC communication, abuse resolution and contact information management.

    - guidance covering formerly regulated services that are moving to unregulated PDNs that have specific requirements in the in-scope networks.

2. Out of Scope for Focus Group 3B:

    - non-US legal issues, private corporate network requirements and operations, inter-provider business or commercial relations and contracts (e.g., peering agreements and financial arrangements), provider Acceptable Use Policies, and users of networks.

    - guidance directed at a specific vendor or service provider or recommendations to use specific vendors or services.

[2] The FCC NRIC VII Designated Federal Officer (DFS) provided an interpretation to the Focus Group during its Meeting No. 7 (July 20-21, 2004 workshop in Washington DC). The DFOs guidance was that better wording for this third deliverable was as follows: "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 service providers that use IP technology in the infrastructures*."

3. In Scope for Focus Group 3B discussion, but should be deferred to other NRIC FG:

   - guidance on general areas, such as power and security that do not have specific concerns for the in-scope networks.

### 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

Network Types included are: Asynchronous Transfer Mode (ATM), Frame Relay (FR), Internet Protocol (IP) and related hybrid or other data protocols.

### 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:[3]

**Service Providers**
An organization that provides services for content providers and for users of a computer network. The services may include access to the computer network, content hosting, server of a private message handling system, news server, etc. 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 operator is responsible for the development, provision and maintenance of real-time networking services and for operating the corresponding networks.

**Equipment Suppliers**
An organization whose business is to supply 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.

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

**Government**
Government includes federal, state and local.

## *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 Public Data 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).

**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 Public Data Networks

Previous Councils have increasingly included both the subject matter of data networks and the related expertise. For example, the Fifth Council included a Subcommittee on Packet Switching Best Practices. This Subcommittee reviewed all existing Best Practices to determine applicability to Pack Switching networks and services. Approximately 97% of the existing Best Practices were found to be applicable; most with some minor refinements or modifications.[4] The Sixth Council also included both a focus and appropriate engagement of data networks expertise. However, this Seventh Council

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

brings an even further level of attention. Recognizing the substantial work available to this Focus Group from the previous Councils, the FCC Designated Federal Officer 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 Public Data Networks.

To ensure healthy rigor in understanding the special needs of Public Data Networks, the Focus Group assembled a list of the attributes that need to be considered. The Focus Group generated a list of over 70 such attributes. A list of attributes of Public Data 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 concerns that could affect the reliability of Public Data 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).

**Figure 2. Analysis of Concerns for Public Data Networks**

### 2.3.2 Best Practices[5]

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.[6]

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

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

Even though NRIC Best Practices have been developed to be easily understood, their essence is often not immediately apparent to those who are inexperienced with the associated job functions.[7] 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

[5] The term "Best Practices" is capitalized when referring to specific NRIC Best Practices.
[6] 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.
[7] Section 7, NRIC V Best Practices Subcommittee Final Report, January 2002. The Keywords provide associations between job functions and Best Practices.

provided to the industry in this document have been demonstrated to be effective, feasible and capable of being implemented.

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

6. Best Practices are verified by a broader set of industry members – from outside the Focus Group – to ensure that those who have not been a part of the process can provide feedback. 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 3B Mission Statement

The Focus Group 3B Mission Statement (Section 2.1.1) specifies 12 specific actions that are to be undertaken by the Focus Group.

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

### 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 fora, government, others). Figure 3, *Public Data Network Networks Focus Group*, 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 Task Group activities described in Section 2.2.

The Focus Group also included a diverse array of disciplines with formal training and experience ranging from mathematics, psychology, field experience, public policy, computer science, human performance, network operations, finance, physics, theology, business management and well as various fields of engineering. In addition, Focus Group members regularly consulted others within their organizations.

**PUBLIC DATA NETWORK RELIABILITY - FOCUS GROUP 3B**

Co-Chair: David Frigeri*, Internap
Co-Chair: Karl F. Rauscher*, Lucent Technologies Bell Labs

**SERVICE PROVIDERS, NETWORK OPERATORS**

| | | | |
|---|---|---|---|
| **ALLTEL** | Scott Binns<br>Tim Hall* | **MCI** | Barry Briggs<br>Mike Diorio |
| **AT&T** | Rick Canaday | **Nextel** | KC Kim* |
| **BellSouth** | Jim L. Johnson | **Qwest** | Brian Rooks |
| **CenturyTel** | Brent Austin<br>Brain White | **Qwest Wireless** | Sherman Phillips |
| **Comcast Cable** | Dean Brewster* | **RCN** | Joe Provo |
| **Cox Communications** | Mark Adams* | **SBC** | John Chapa<br>Ren Provo |
| **Equinix** | William Norton | **Sprint** | Chase Cotton* |
| **Global Crossing** | David Cooper | **Telefonica** | Dennis Di Toro<br>William Groh |
| **Ibasis** | Solos Arthachinda<br>Ajay Joseph | **Time Warner Cable** | Ron da Silva |
| **Internap** | Duke McMillin*<br>Jon Vestal | **Verisign** | Ken Silva |
| **Intelsat** | Mark Neibert | **Verizon** | Robin Howard |

**EQUIPMENT SUPPLIERS**

| | | | |
|---|---|---|---|
| **Cisco Systems** | Robin Roberts | **Marconi** | Brad Nelson* |
| **Juniper Networks** | Fred Stringer | **Nortel Networks** | Srini Anam |
| **Lucent Technologies** | Richard Krock*<br>James P. Runyon | **SpectraSite** | Ted Abrams |

**OTHERS**

| | | | |
|---|---|---|---|
| **ATIS** | Bill Klein (A) | **FCC** | Jeff Goldthorp (A)<br>Kent Nilsson (A) |
| **CAIDA** | K Claffy | **Harvard University** | Scott Bradner |
| **CTIA** | Rick Kemper | **SAIC** | Hank Kluepfel (A) |

**Figure 3. Public Data Network Reliability Focus Group**
*Task Group Leaders, (A) Advisors

#### 2.3.4.2 Activities

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

### 2.3.5 Approach

The Focus Group's approach to fulfill its Mission was based on the steps of assembling sufficient expertise and diversity of perspectives, generating a list of PDN attributes, developing a list of concerns from this list of attributes and the assembled expertise and then conducting analysis to determine if the known concerns are covered by existing, document NRIC Best Practices. To do this, several meetings were dedicated to brainstorming and rigorous discussion with respect to the following areas:

The attributes of PDN and Internet Service Provider Networks
- Over 70 PDN and ISP attributes were identified by this activity (Appendix 5)

The issues and problems faced by PDNs and Internet Service Providers
- Over 200 issues and problems were identified by this activity

Priority topics that the PDN Focus Group should consider
- 11gaps were identified

Using the 8 dimensions of the communications infrastructure identified in the Figure 4, the Focus Group formed Task Groups. The PDN and ISP attributes, issues and problems, and priority topics were distributed across these Task Groups, as appropriate.

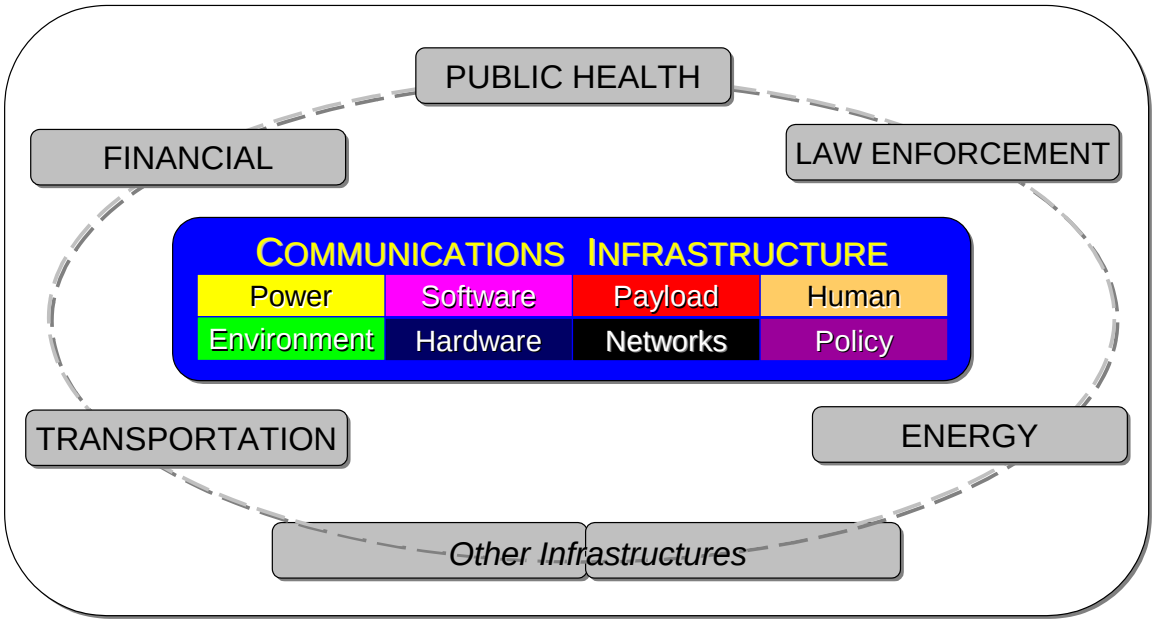


**Figure 4. Communications Infrastructure[8]**

[8] From NRIC VI Homeland Security Physical Security Focus Group.

The Task Group and Leaders are as follows:

- Environment Task Group – Dean Brewster, Comcast Communications
- Hardware Task Group – Tim Hall, ALLTEL; Karl Rauscher, Lucent Technologies Bell Labs
- Human Task Group – KC Kim, Nextel Communications
- Network Task Group – Mark Adams, Cox Communications
- Payload Task Group - David Frigeri, Internap Network Services
- Policy Task Group – Chase Cotton, Sprint
- Power Task Group – Rick Krock, Lucent Technologies
- Software Task Group – Brad Nelson, Marconi

#### 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 | ~500 |
| Workshops | ~1000 |
| Total | ~1500 |

Table 3 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 of these meetings lasted 2 days.

| MEETING NUMBER | DATE | MEETING TYPE | PARTICIPANTS |
|---|---|---|---|
| 1 | May 13, 20024 | Conference Call | 26 |
| 2 | May 21, 2004 | Conference Call | 20 |
| 3 | May 25, 2004 | Workshop (DC) | 16 |
| | May 26, 2004 | Workshop (DC) | 16 |
| 4 | June 7, 2004 | Conference Call | 19 |
| 5 | June 25, 2004 | Conference Call | 19 |
| 6 | July 16, 2004 | Conference Call | 19 |
| 7 | July 20, 2004 | Workshop (DC) | 14 |
| | July 21, 2004 | Workshop (DC) | 13 |
| 8 | August 3, 2004 | Conference Call | 15 |
| 9 | August 25, 2004 | Conference Call | 21 |
| 10 | September 8, 2004 | Workshop (DC) | 15 |
| | September 9, 2004 | Workshop (DC) | 13 |
| 11 | September 20, 2004 | Conference Call | 16 |
| 12 | October 4, 2004 | Workshop (DC) | 15 |
| | October 5, 2004 | Workshop (DC) | 13 |
| 13 | October 18, 2004 | Conference Call | 13 |
| 14 | November 3, 2004 | Workshop (DC) | 8 |
| | November 4, 2004 | Workshop (DC) | 10 |
| 15 | November 8, 2004 | Conference Call | 10 |
| 16 | November 9, 2004 | Conference Call | 11 |
| 17 | November 10, 2004 | Conference Call | 12 |
| 18 | November 11, 2004 | Conference Call | 13 |
| 19 | November 12, 2004 | Conference Call | 11 |
| 19 | November 15, 2004 | Conference Call | 7 |

**TABLE 3. Focus Group Meetings and Participation**

#### 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:[9]

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

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 Telecommunications and Information Administration (NTIA)
- North American Network Operators' Group (NANOG)
- 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)

### 2.3.7 Other Focus Groups

Because of the common areas of subject matter, the Public Data Networks 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 10 gaps identified by this Focus Group were distributed across the communications infrastructure areas as shown in Table 4.

**TABLE 4. Distribution of Identified Gaps**

| Area | Number of Gaps | Section |
|---|---|---|
| Environment | 1 | 3.2.1 |
| Hardware | 0 | 3.2.2 |
| Human | 0 | 3.2.3 |
| Network | 3 | 3.2.4 |
| Payload | 0 | 3.2.5 |
| Policy | 0 | 3.2.6 |
| Power | 2 | 3.2.7 |
| Software | 4 | 3.2.8 |

## 3.2 Task Group Analysis

### 3.2.1 ENVIRONMENT

#### 3.2.1.1 Subject Matter

Everything needs to be somewhere. Environment includes a wide range of areas such as buildings, tower sites, satellite glide paths, cable trenches, ocean floors and overhead lines. Communications infrastructure is virtually everywhere.

Some environments present many challenges to communications equipment. Considerations such as temperature, fire, contaminates, floods, ice, snow, and animals such as avian and rodents are addressed in this area. Some factors related to the environment can be controlled or mitigated and some cannot, making the task of protecting communications infrastructure an incredible challenge.

The Environment Task Group reviewed reliability considerations of Public Data Networks by addressing the design, planning, construction, growth, access, and operations related to environments.

#### 3.2.1.2 Task Group Participants

The Environment Task Group assembled a diverse team of 9 individuals with representatives that include equipment suppliers, network and service providers. In addition to members of the Task Group, subject matter experts were engaged to strengthen its expertise and develop proposed Best Practices. Table 5 lists the Environment Task Group participants.

**TABLE 5. Environment Task Group Participants**

| Name | Organization |
|---|---|
| Victor DeVito | AT&T |
| Dean Brewster, **Leader** | Comcast Corporation |
| Ray Cruz | Internap Network Services |
| Jim Runyon | Lucent Technologies, Bell Labs |
| Rick Krock | Lucent Technologies, Bell Labs |
| Brad Nelson | Marconi |
| Brian Rooks | Qwest Communications |
| Molly Schwarz | Schwarz Consulting |
| Chase Cotton | Sprint |

#### 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 [Public Data Networks] providers are needed*."

As a starting point and to encourage free form and innovative thinking the Focus Group and Environment Task Group used brainstorming and analysis methods or submittals by industry experts to detail a listing of 9 potential concerns for the environment area of Public Data Networks.

The 9 potential concerns were subsequently analyzed by the Environment Task Group to determine if they were applicable to Public Data Networks and a potential candidate for a Best Practice Guidance. Through this analysis, the original list was consolidated into a more concise grouping of 5 potential concerns. These concerns have been undergoing detailed analysis and a review against current Best Practices to determine the proper disposition. These 5 concerns were determined to be: 1) addressed by existing Best Practices, 2) transferred to the Homeland Security Infrastructure Focus Group, or 3) identified as gaps for Public Data Network reliability.

**Managing Growth in Multi-Tenant Facilities**

The Environment Task Group identified one gap in existing, documented NRIC Best Practices related to the complexity of managing growth in third party and multi-tenant environments (e.g., space, power, cooling).

Work continues in this area to define Best Practices. Further analysis and industry research will continue to bring new ideas forward. Existing Best Practices will continue to be reviewed and gap analysis will be performed.

## 3.2.2 HARDWARE

### 3.2.2.1 Subject Matter

Hardware plays a fundamentally critical role in the reliability of Public Data Networks. The Hardware Area includes the broad category of physical electronics and related components that are part of communications systems. Hardware systems include: frames, racks, cabinets, chasses; circuit packs, cards, blades, plug-ins and modules; fiber optic transmission facilities; cables (with exception to the power systems; and, power distribution systems such as fuse panels which was addressed in the Power Section 3.2.7). The electronic hardware equipment includes switches, routers, multiplexing equipment, transmission equipment, access equipment, satellites, dishes, undersea cables, microwave repeaters, cell sites, etc. There are on the order of tens of thousands of routers and switches from multiple equipment suppliers deployed in U.S. public networks. These network elements range in size from something as small as cereal box to complexes of more than 10 cabinets. Sometimes a carrier hotel contains many service providers using switches and routers from many different equipment suppliers.[10]

### 3.2.2.2 Task Group Participants

The Hardware Task Group assembled a team of sufficient expertise to effectively address the Hardware subject matter as it relates to the reliability of public data networks. The Hardware Task Group was made up of 13 participants. In addition to members of the Focus Group, the Task Group engaged other subject matter experts to strengthen its expertise. The primary hardware disciplines of physics, chemistry and electrical engineering were represented on the team. 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 |
|---|---|
| Tim Hall, ***Leader*** | ALLTEL |
| Jim Johnson | BellSouth |
| Robin Roberts | Cisco Systems |
| Mark Adams | Cox Communications |
| Scott Bradner | Harvard University |
| Duke McMillan | Internap Network Services |
| Fred Stringer | Juniper Networks |
| Brad Nelson | Marconi Corporation |
| KC Kim | Nextel Communications |
| Rick Krock | Lucent Technologies |
| Theodore Lach | Lucent Technologies |
| Karl Rauscher, ***Leader*** | Lucent Technologies, Bell Labs |
| Hank Kluepfel | SAIC |

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

### 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 Data Networks providers are needed." As described in Section 2.3.5, the approach used for Hardware was similar for the other areas. Therefore, a gap is here defined as a space between the known problems associated with Hardware that can impact network reliability and the existing NRIC Best Practices for Hardware. To understand the former boundary, a list was generated of 19 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 Data Networks.[11] In addition, the Task Group reviewed the work of the previous Council in which the vulnerabilities of Hardware were systematically reviewed. [12, 13]

The Task Group's gap analysis determined that there were no significant gaps in the Hardware area.[14] Several minor refinements have been proposed for the existing Best Practices, and these are under consideration and may yield further discussion in a future issue of this report.

---

[11] 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.

[12] Vulnerability: *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.

[13] The Homeland Security Physical Security Focus Group (1A) of NRIC VI carefully listed the *categories* of hardware vulnerability as chemical, physical, electromagnetic, environmental and life cycle (aging). The specific vulnerabilities include corrosion, temperature, shock, vibration, physical destruction, radiation and aging. These vulnerabilities, if exercised by a threat, can shorten the life or cause intermittent malfunctioning of hardware systems, or in the extreme, shut them down. See NRIC VI Homeland Security Physical Security Focus Group Final Report, Issue, 3, December 2003, p. 49.

[14] The Task Group recognized that there were 4 Hardware Areas for Attention identified by the previous Council's Homeland Security work. Specifically, 3 areas dealing with susceptibility to radiation (nuclear attack, hardening for radiation, and solar flare and coronal mass ejection), and a fourth that identified the increasing challenge of maintaining control of the hardware development process amidst growing outsourcing. The Task Group recognizes these Areas for Attention for Homeland Security, but does not see them as specific Public Data Networks.

### 3.2.3 HUMAN

#### 3.2.3.1 Subject Matter

The Human factor has a critical role in the reliability of public data networks. This area includes both employees and employers of network operators, carriers, vendors, government, and property managers who are associated with the development, deployment and management of Public Data Network. All network-related problems have the potential of being caused by or affected by human interaction. Items considered within the Human area include preventing human errors, protecting humans, the tendency of human deterrence to change, sharing human experiences, determining sound processes and procedures, providing training, educating customers, and sharing proper information within the society. There are *over 1,000,000 people* working in various size companies associated with U.S. Public Data Networks. An organization's size, structure and culture play important roles in determining exposure of Public Data Networks to human vulnerabilities.

#### 3.2.3.2 Task Group Participants

The Human Task Group assembled a team of sufficient expertise to effectively address the Human subject matter as it relates to the reliability of public data networks. The Human Task Group was made up of 5 participants. In addition to members of the Focus Group, the Task Group engaged other subject matter experts to strengthen its expertise. Table 7 lists the Human 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 7. Human Task Group Participants**

| Name | Organization |
|---|---|
| Jon Vestal | Internap Network Services |
| Michael Diorio | MCI |
| Anil Macwan | Lucent Technologies |
| KC Kim, ***Leader*** | Nextel |
| Ren Provo | SBC |

#### 3.2.3.3 Gap Analysis

The Council Charter directs the Focus Group to "*perform a gap analysis to determine areas where new Best Practices for [Public Data Networks] providers are needed*." As described in Section 2.3.5, the approach used for Human was similar for the other areas. Therefore, a gap is defined as space between the known problems associated with Humans that can impact network reliability and the existing Best Practices. To understand the former boundary, a list was generated of 8 potential areas of concerns for the Human factor. To understand the latter boundary, the existing Best Practices were researched and 90 Best Practices were found to have potential application to the reliability of public data networks.[15] In addition, the Task Group reviewed the work of the

[15] An NRIC Best Practices web site keyword search for "human" returns the following 9 Best Practices: 6-5-0561, 6-5-0564, 6-5-0650, 6-5-0678, 6-5-0746, 6-5-5027, 6-5-5059, 6-5-5061, 6-6-

previous Council in which the Human vulnerabilities were systematically reviewed. We analyzed each of the concerns in light of the existing Best Practices to find any gaps.

The gap analysis determined that there were no significant gaps in the Human area. Several refinements have been proposed for existing Best Practices. These are under consideration and may yield further modifications in a future issue of this report.

---

5086. An NRIC Best Practices web site keyword search for “employee” returns the following 20 Best Practices: 6-5-0542, 6-5-0570, 6-5-0598, 6-5-0697, 6-5-0716, 6-6-1016, 6-6-1018, 6-6-1038, 6-6-5015, 6-6-5016, 6-6-5019, 6-6-5033, 6-6-5037, 6-6-5115, 6-6-5164, 6-6-5244, 6-6-8098, 6-6-8100, 6-6-8519, 6-6-8521. An NRIC Best Practices web site keyword search for ”training” returns the following 61 Best Practices: 6-5-0511, 6-5-0537, 6-5-0564, 6-5-0565, 6-6-0577, 6-5-0578, 6-5-0579, 6-5-0588, 6-5-05896-5-0597, 6-5-0598, 6-6-0599, 6-5-0629, 6-5-0650, 6-5-0697, 6-5-0711, 6-5-0713, 6-5-0729, 6-6-1001, 6-6-1019, 6-6-1035, 6-6-1036, 6-6-1057, 6-6-3212, 6-6-5015, 6-6-5019, 6-6-5021, 6-6-5023, 6-6-5027, 6-6-5054, 6-6-5055, 6-6-5067, 6-6-5091, 6-6-5093, 6-6-5094, 6-6-5114, 6-6-5115, 6-6-5116, 6-6-5126, 6-6-5138, 6-6-5139, 6-6-5155, 6-6-5175, 6-6-5178, 6-6-5179, 6-6-5184, 6-6-5203, 6-6-5208, 6-6-5217, 6-6-5244, 6-6-5266, 6-6-5267, 6-6-5269, 6-6-5270, 6-6-8062, 6-6-8067, 6-6-8082, 6-6-8097, 6-6-8100, 6-6-8517, 6-6-8519

## 3.2.4 NETWORK

### 3.2.4.1 Subject Matter

A Network is defined as a series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain sub-networks. The networks that support the United States communications infrastructure are immense both in terms of communications services provided and geographic coverage. Networks are designed with capabilities that minimize or mitigate the impact of failures on the services provided. A public data network is for the specific purpose of providing data transmission services for the public. At the Network Task Group level, environment, power, hardware, software, human, procedure and policy must all come together to form a reliable communications infrastructure. The Network Task Group is focused on improving the reliability of the Public Data Network by addressing the design and planning, provisioning, operational, administration and maintenance aspects of network performance:

**Design and Planning:** The activities associated with building, expanding or modifying a network. Examples include capacity management, planning and implementing network design, engineering, new facilities and routes.

**Provisioning:** The creation or modification of parameters of a subscriber account. Provisioning of a subscriber account includes subscriber account registration and device activation.

**Operations:** The day-to-day activities associated with keeping a network operating reliably and efficiently. Examples include traffic management, circuit grooming and other activities centered on improving or ensuring network performance.

**Administration:** Administration includes all activities associated with managing a network from a business, network and information technology perspective (e.g., billing, IP address administration, databases).

**Maintenance:** The ongoing corrective or preventive activities associated with keeping the network operating including planned and unplanned maintenance. Planned maintenance is for network enhancements or action to prevent network disruptions. Unplanned maintenance is an unexpected network activity.

### 3.2.4.2 Task Group Participants

The Network Task Group assembled a diverse team of 7 individuals with representatives that include equipment suppliers, network/service providers and academia. 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 |
|---|---|
| Tim Hall | ALLTEL |
| Rick Canaday | AT&T |
| Mark Adams, ***Leader*** | Cox Communications |
| Dave Cooper | Global Crossing |
| Scott Bradner | Harvard University |
| Jim Runyon | Lucent Technologies, Bell Labs |
| John Chappa | SBC |

### 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 [Public Data Networks] providers are needed*."

As a starting point and to encourage free form and innovative thinking the 3B Focus Group and Network Task Group used brainstorming methods and submittals by industry experts to detail a listing of 71 new, potential concerns for the network area of Public Data Networks.

The 71 potential concerns were subsequently analyzed by the Network Task Group to determine if they were applicable to Public Data Networks and a potential candidate for a best practice. Through this analysis, the original list was consolidated into a more concise grouping of 40 potential concerns. Each potential issue on the list of 40 has been undergoing detailed analysis and review to determine proper disposition:

- addressed by an existing Best Practice
- out of scope or not applicable to Public Data Networks
- consolidate with other potential issues on the list
- transferred to another Task Group
- Best Practice candidate.

Three gaps have been identified:

**Network Design and Planning**

73 Best Practices currently exist relative to network design. The Task Group has identified opportunities to enhance NRIC Best Practices in the following areas: the treatment of private address space, routing practice, and design audit.

**Network Measurement and Management**

One Best Practice exists relative to Equipment Suppliers measuring and improving quality. The Task Group has identified opportunities to expand and clarify the scope of the Best Practice to include Service Providers and Network Operators.

**Network Spares Administration**

At least 12 current Best Practices touch on spare equipment. The Task Group has identified an opportunity to improve guidance in the area of spares management.

**Maintenance Window**

One current Best Practice exists for the definition of maintenance windows. The Task Group has identified an opportunity to improve guidance in the communication of maintenance timeframes.

Existing Best Practices[16] will be modified and new Best Practices will be developed, as appropriate.

[16] NRIC Best Practices web site keyword searches touching the network area resulted in the following: Reliability: 261 Procedural: 204 Network Operations: 151 Network Design: 73 Network Provisioning: 56 Technical Support: 51.

## 3.2.5 PAYLOAD

### 3.2.5.1 Subject Matter

Payload includes any messages that go across networks. The Payload in Public Data Networks, typically thought of as the data associated with end-user applications, is increasingly becoming an essential element in the continued operation of our nation's communications infrastructure. Payload, whether data, image, video, or voice, is rapidly becoming a major source of communication as well as a major component of information, news, entertainment, commerce, public safety, transportation, national security, and emergency response.

Payload in the sense of Public Data Networks most commonly refers to the data contained inside the IP packet within the TCP/IP protocol suite. The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another across any IP enabled network, although we will generically use Internet within this report. When an end-user's application sends or receives data (e.g., an e-mail note or a Web page), the message gets divided into little chunks of data called packets. Each of these packets of data also contains both the sender's Internet address and the receiver's address. Packets are sent first to a router that understands a small part of the Internet then passes the packet onto subsequent routers until the packet reaches the destination.

Unlike circuit switch networks, IP is a connectionless protocol, which means that there is no fixed path or continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. The most widely used version of IP today is Internet Protocol Version 4 (IPv4). However, IP Version 6 (IPv6) is also beginning to be supported.

### 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 |
|---|---|
| Solos Arthachinda | IBasis |
| Ajay Joseph | IBasis |
| David Frigeri, ***Leader*** | Internap Network Services |
| Manny Sidhu | Internap Network Services |
| Jon Vestal | Internap Network Services |
| Jim Runyon | Lucent Technologies, Bell Labs |

#### 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 [Public Data Networks] providers are needed*." As described in Section 2.3.5, the approach used for Payload was similar for the other areas. 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 30 known concerns for Payload. To understand the latter boundary, the existing Best Practices were researched and 48 were found to have potential application to Public Data Network reliability.[17] In addition, the Task Group reviewed the work of the previous Council in which the vulnerabilities of payload were systematically reviewed.[18] [19]

The Task Group's gap analysis determined that there were no significant gaps in the Payload area. Several minor refinements have been proposed for the existing Best Practices, and these are under consideration and may yield further discussion in a future issue of this report.

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

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

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

## 3.2.6 POLICY

### 3.2.6.1 Subject Matter

The Policy area includes agreements between multiple parties such as industry standards, industry practices, and industry interfaces both physical and logical, e.g. protocols. The Internet, like many other Public Data Networks, is formed of many networks owned and operated independently by a large number of service providers. Continued success in providing a high reliability service offering over a network formed of multiple administrative domains clearly depends upon industry agreement on good operating methods, procedures, and common protocol suites.

Practices associated with the Policy area have a critical role in the reliability of the Internet. The transport of an end customer's IP (Internet Protocol) datagrams across the Internet (commonly called IP "transit") depends upon both the family of IP protocol standards and a common industry framework of how addressing and routing should happen.

The Policy Task Group considered the following areas specifically related to Internet Service Providers:

- Addressing - Mechanisms for management of a provider's addresses and address spaces
- Naming - Mechanisms associated with the Domain Name System (DNS) and the mapping between IP addresses and domain names
- Routing - Mechanisms for maintaining a provider's network topology and distribution of prefixes (routes) internally[20]
- Interconnection - Mechanisms for exchanging routes between providers
- Abuse - Mechanisms for dealing with network abuse (DOS, SPAM, etc.)

The Policy Task Group believes this taxonomy broadly covers the current practice space associated with design, engineering, and operations in modern Internet Service Providers. The Policy Task Group also considered several additional practice areas, not specifically related to Internet Service Providers, but having general application to all Public Data Network operators:

- Network Management - Mechanisms for element and overall network management, provisioning, and surveillance[21]
- Service Assurance (sometimes called Service Delivery) - Ongoing management of customer's services[22]
- Provider-Customer - Interactions and mechanisms between a provider and a customer
- Inter-Provider - Interactions and mechanisms between two providers

[20] These items will be moved to the Network Task Group area in subsequent issues of this report
[21] Ibid.
[22] Ibid.

The Policy Task Group reviewed existing Best Practices against these Policy areas and other common industry practices and keywords and found reasonable coverage of Internet Service Provider topics:

- Internet 27[23]
- IP (Internet Protocol) 20[24]
- routing 33[25] (not all IP-specific)
- peering 10[26]
- CIDR (Classless Inter-Domain Routing) 1[27]
- domain, DNS (Domain Name System) 8[28], 13[29]
- BGP (Border Gateway Protocol) 6[30]
- service assurance 2[31]
- inter-provider 0
- SLA (Service Level Agreement) 4[32]
- QoS (Quality of Service) 2[33]
- ISP (Internet Service Provider) 16[34]
- RFC (Request For Comments) 16[35]
- AUP (Acceptable Use Policy) 4[36]
- SPAM 1[37]
- DOS (Denial of Service) 12[38] (not all Internet-specific)

---

[23] see NRIC Best Practices 6-5-0506, 6-5-0508, 6-5-0608, 6-6-3210, 6-6-5068, 6-6-8008, 6-6-8015, 6-6-8029, 6-6-8043, 6-6-8046, 6-6-8047, 6-6-8048, 6-6-8051, 6-6-8052, 6-6-8068, 6-6-8070, 6-6-8077, 6-6-8079, 6-6-8080, 6-6-8081, 6-6-8083, 6-6-8086, 6-6-8090, 6-6-8093, 6-6-8525, 6-6-8527, 6-6-8528

[24] see NRIC Best Practices 6-5-0506, 6-5-0507, 6-5-0508, 6-5-0516, 6-5-0533, 6-6-0762, 6-6-0764, 6-6-0765, 6-6-0769, 6-6-8040, 6-6-8043, 6-6-8051, 6-6-8055, 6-6-8056, 6-6-8057, 6-6-8090, 6-6-8106, 6-6-8522, 6-6-8535, 6-6-8539

[25] see NRIC Best Practices 6-5-0500, 6-5-0510, 6-5-0516, 6-5-0519, 6-5-0520, 6-5-0524, 6-5-0526, 6-5-0566, 6-5-0568, 6-5-0570, 6-5-0572, 6-5-0579, 6-5-0603, 6-5-0617, 6-5-0618, 6-5-0622, 6-5-0651, 6-5-0679, 6-5-0709, 6-5-0727, 6-5-0731, 6-6-5107, 6-6-8041, 6-6-8042, 6-6-8043, 6-6-8045, 6-6-8049, 6-6-8050, 6-6-8108, 6-6-8525, 6-6-8526, 6-6-8531, 6-6-8565

[26] see NRIC Best Practices 6-5-0503, 6-5-0524, 6-6-0806, 6-6-8040, 6-6-8042, 6-6-8043, 6-6-8044, 6-6-8050, 6-6-8093, 6-6-8525

[27] see NRIC Best Practices 6-5-0503

[28] see NRIC Best Practices 6-5-0510, 6-6-8015, 6-6-8046, 6-6-8047, 6-6-8048, 6-6-8089, 6-6-8527, 6-6-8528

[29] see NRIC Best Practices 6-5-0510, 6-5-0523, 6-6-0762, 6-6-0763, 6-6-8042, 6-6-8043, 6-6-8044, 6-6-8046, 6-6-8047, 6-6-8048, 6-6-8525, 6-6-8527, 6-6-8528

[30] see NRIC Best Practices 6-5-0516, 6-6-8042, 6-6-8043, 6-6-8044, 6-6-8050, 6-6-8525

[31] see NRIC Best Practices 6-5-0530, 6-5-0547

[32] see NRIC Best Practices 6-6-0802, 6-6-0811, 6-6-8504, 6-6-8506

[33] see NRIC Best Practices 6-5-0521, 6-6-0811

[34] see NRIC Best Practices 6-5-0502, 6-6-5068, 6-6-8042, 6-6-8043, 6-6-8044, 6-6-8050, 6-6-8066, 6-6-8078, 6-6-8079, 6-6-8080, 6-6-8092, 6-6-8093, 6-6-8513, 6-6-8514, 6-6-8525, 6-6-8531

[35] see NRIC Best Practices 6-5-0515, 6-5-0516, 6-5-0617, 6-6-0763, 6-6-0764, 6-6-0765, 6-6-0767, 6-6-0768, 6-6-8046, 6-6-8047, 6-6-8048, 6-6-8050, 6-6-8070, 6-6-8527, 6-6-8528, 6-6-8531

[36] see NRIC Best Practices 6-5-0533, 6-6-8092, 6-6-8514, 6-6-8521

[37] see NRIC Best Practice 6-5-0533

[38] see NRIC Best Practices 6-5-0506, 6-5-0533, 6-6-8043, 6-6-8053, 6-6-8074, 6-6-8075, 6-6-8076, 6-6-8523, 6-6-8528, 6-6-8530, 6-6-8533, 6-6-8561

#### 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 Internet Service providers and public data networks. The Task Group was made up of 7 participants. In addition to members of the Focus Group, the Task Group engaged other subject matter experts to strengthen its expertise. The primary disciplines of network architecture, design, engineering, operations, standards, measurement, and testing were represented on the team. Table 10 lists the Policy Task Group participants. Care was also taken to include representation from a broad range of industry roles. The team had sufficient expertise to complete this activity.

**TABLE 10. Policy Task Group Participants**

| Name | Organization |
|---|---|
| K. Claffy | CAIDA |
| Dean Brewster | Comcast |
| William B. Norton | Equinix |
| Scott Bradner | Harvard University |
| Brian Rooks | Qwest |
| Chase Cotton, ***Leader*** | Sprint |
| Ren Provo | SBC Internet Services |

#### 3.2.6.3 Gap Analysis

The Council Charter directs the Focus Group to "*perform a gap analysis to determine areas where new Best Practices for [Public Data Networks] providers are needed*." As described in Section 2.3.5, the approach used for Policy was similar for the other areas. Therefore, a gap is here defined as a space between the known problems associated with the Policy area that can impact network reliability and the existing Best Practices for Policy.

The Policy Task Group's gap analysis determined that there were no significant gaps in the Policy area. The Policy Task Group's gap analysis did however determine that there are a number of opportunities to refine or modify existing Best Practices to provide better coverage for Public Data Networks. Possible refinements that the Task Group will be consider are in the areas of: address space documentation and management, Domain Name System (DNS), element configuration practice, route exchange practice, and nominal abuse practices, security of network management, and inter-provider communications.

## 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.[39] Power is an essential basic element of the communications infrastructure, without which networks will not function. In addition, any power problem has the potential to become a catastrophe, potentially damaging other equipment and personnel.[40]

### 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 Public Data Networks. The Power Task Group was made up of 7 participants. Network Operators, Power Equipment Manufactures, communications Equipment Suppliers and academia 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 |
|---|---|
| Harold Washer | BatteryCorp |
| Dean Brewster | Comcast Communications |
| Scott Bradner | Harvard University |
| Ray Cruz | Internap Network Services |
| Rick Krock, ***Leader*** | Lucent Technologies, Bell Labs |
| Jim Runyon | Lucent Technologies, Bell Labs |
| Chase Cotton | Sprint |

### 3.2.7.3 Gap Analysis

The Council Charter directs the Focus Group to "*… perform a gap analysis to determine areas where new Best Practices for [Public Data Networks] providers are needed*." In addition, *"The Council shall focus on the special needs of the Public Data Network industry and refine existing Best Practices to focus their applicability to the Public Data Network industry."* As described in Section 2.3.5, the approach used for Power was similar for the other areas. Therefore, a gap is here defined as a space between the known problems associated with power that can impact the Public Data Network reliability and the existing Best Practices for power. To understand the former boundary, a list of 10 concerns related specifically to power in public data networks was generated. To understand the latter boundary, the existing 101[41] Best Practices pertaining to power

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

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

[41] 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-

were researched. The concerns were identified as being adequately addressed by existing Best Practices, transferred to the Network Task Group, or identified as gaps. The Task Group identified two gaps. One gap deals with proper identification of cables, and the other deals with back-up power for on-premise emerging data services equipment.

**Proper Identification of Cables**
Administration, maintenance and operations of network elements depend on proper identification of equipment. While there are numerous Best Practices that address administration, operations and maintenance, and while Network Operators currently employ various effective methods of cable labeling, the NRIC Best Practices do not document guidance in this area.

**Back-Up Power for On-Premise Emerging Data Services Equipment**
Emerging data services, such as Voice Over IP (VoIP) are increasingly viewed as critical services. As such, this equipment may need to continue to function even during commercial power outages. Because the end user equipment is increasingly powered by local sources, back-up power consideration should be explored. As these networks are still very new, further analysis is pending.

These 2 gaps are being reviewed by the Focus Group to determine whether existing Best Practices can be revised or whether new Best Practices can be developed to address these concerns.

---

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

## 3.2.8 SOFTWARE

### 3.2.8.1 Subject Matter

Software has a critical role in the reliability of Public Data Networks. The Software area includes the broad category of operating systems, applications, and firmware that are part of a communications system. Software spans switches, routers, transport equipment, transmission equipment, access equipment, satellites, dishes, undersea cables, microwave repeaters, cell sites, PCs, and end user devices. Many of the routers and switches from multiple equipment suppliers employ Software Defined Networks such as Virtual Private Networks. The number of lines of code in the communications networks in the United States is on the order of hundreds of millions. Both network and systems engineers rely heavily on Network Management software and software services to operate and maintain their networks. Despite the diversity of hardware in use in the public networks, there is a wide variety of agreed upon software standards available and in use that allow interoperability and manageability.

### 3.2.8.2 Task Group Participants

The Software Task Group assembled a team of sufficient expertise to effectively address the Software subject matter as it relates to the reliability of public data networks. The Software Task Group was made up of 10 participants. In addition to members of the Focus Group, the Task Group engaged other subject matter experts to strengthen its expertise. The primary Software disciplines were represented on the team. Table 12 lists the Software 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 12. Software Task Group Participants**

| Name | Organization |
|---|---|
| Robin Roberts | Cisco Systems |
| Jon Vestal | Internap Network Services |
| Duke McMillan, ***Leader*** | Internap Network Services |
| Jim Filreis | Internap Network Services |
| Fred Stringer | Juniper Networks |
| Art Morrical | Lucent Technologies |
| Jim Runyon | Lucent Technologies, Bell Labs |
| Paul Wolfson | Lucent Technologies |
| Brad Nelson, ***Leader*** | Marconi |
| Mike Kennedy | Nortel |

### 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 [Public Data Networks] providers are needed*." As described in Section 2.3.5, the approach used for Software was similar for the other areas. Therefore, a gap is here defined as a space between the problems associated with Software that can impact network reliability and the existing NRIC Best Practices for Software.

To understand the former boundary, a list was generated of 42 concerns for Software. Upon further review and comparison to 216 existing NRIC Best Practices,[42] the Task Group has identified four (4) gaps spanning the following areas:

**Management Information Base (MIB)[43]**

Due to the quantity and interactions of "private" MIB extensions with proprietary and other management software, the Task Group has identified opportunities to enhance NRIC Best Practices in the areas of MIB support, standardization, and documentation. In addition, there is opportunity to improve support of environmental variables in MIBs.

**Crash Diagnostic Memory**

The Task Group has identified opportunities to enhance NRIC Best Practices in the area of crash diagnostic memory storage and the use non-volatile memory. There is added opportunity to improve storage of core dumps and system states associated with a crash.

**Software Configuration**

---

[42] 6-5-0500, 6-5-0506, 6-5-0507, 6-5-0523, 6-5-0533, 6-5-0535, 6-5-0536, 6-5-0537, 6-5-0538, 6-5-0541, 6-5-0550, 6-5-0551, 6-5-0552, 6-5-0553, 6-5-0554, 6-5-0555, 6-5-0557, 6-5-0559, 6-5-0585, 6-5-0590, 6-5-0600, 6-5-0601, 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, 6-6-0806, 6-6-0807, 6-6-0808, 6-6-0809, 6-6-0811, 6-6-0813, 6-6-1003, 6-6-1005, 6-6-5061, 6-6-5084, 6-6-5121, 6-6-5142, 6-6-5165, 6-6-5167, 6-6-5172, 6-6-5200, 6-6-5218, 6-6-5219, 6-6-5254, 6-6-5276, 6-6-5277, 6-6-5278, 6-6-5279, 6-6-8000, 6-6-8001, 6-6-8002, 6-6-8003, 6-6-8004, 6-6-8005, 6-6-8006, 6-6-8007, 6-6-8008, 6-6-8009, 6-6-8010, 6-6-8011, 6-6-8012, 6-6-8013, 6-6-8014, 6-6-8015, 6-6-8016, 6-6-8017, 6-6-8018, 6-6-8019, 6-6-8020, 6-6-8021, 6-6-8022, 6-6-8023, 6-6-8024, 6-6-8025, 6-6-8026, 6-6-8027, 6-6-8028, 6-6-8029, 6-6-8030, 6-6-8031, 6-6-8032, 6-6-8033, 6-6-8034, 6-6-8035, 6-6-8036, 6-6-8037, 6-6-8038, 6-6-8039, 6-6-8040, 6-6-8041, 6-6-8042, 6-6-8043, 6-6-8044, 6-6-8045, 6-6-8046, 6-6-8047, 6-6-8048, 6-6-8049, 6-6-8050, 6-6-8051, 6-6-8052, 6-6-8053, 6-6-8054, 6-6-8055, 6-6-8056, 6-6-8057, 6-6-8058, 6-6-8059, 6-6-8060, 6-6-8061, 6-6-8062, 6-6-8063, 6-6-8064, 6-6-8065, 6-6-8066, 6-6-8067, 6-6-8068, 6-6-8069, 6-6-8070, 6-6-8071, 6-6-8072, 6-6-8073, 6-6-8074, 6-6-8075, 6-6-8076, 6-6-8077, 6-6-8078, 6-6-8079, 6-6-8080, 6-6-8081, 6-6-8082, 6-6-8083, 6-6-8084, 6-6-8085, 6-6-8086, 6-6-8087, 6-6-8088, 6-6-8089, 6-6-8090, 6-6-8091, 6-6-8092, 6-6-8093, 6-6-8094, 6-6-8095, 6-6-8096, 6-6-8097, 6-6-8098, 6-6-8099, 6-6-8100, 6-6-8101, 6-6-8102, 6-6-8103, 6-6-8104, 6-6-8105, 6-6-8106, 6-6-8108, 6-6-8109, 6-6-8110, 6-6-8500, 6-6-8501, 6-6-8502, 6-6-8503, 6-6-8504, 6-6-8505, 6-6-8506, 6-6-8507, 6-6-8508, 6-6-8509, 6-6-8510, 6-6-8513, 6-6-8514, 6-6-8515, 6-6-8517, 6-6-8519, 6-6-8521, 6-6-8522, 6-6-8523, 6-6-8525, 6-6-8526, 6-6-8527, 6-6-8528, 6-6-8530, 6-6-8531, 6-6-8532, 6-6-8533, 6-6-8534, 6-6-8535, 6-6-8537, 6-6-8539, 6-6-8540, 6-6-8548, 6-6-8549, 6-6-8551, 6-6-8553, 6-6-8554, 6-6-8555, 6-6-8556, 6-6-8557, 6-6-8559, 6-6-8561, 6-6-8562, 6-6-8563, 6-6-8564, 6-6-8565, 6-6-8566, 6-6-8567

[43] A MIB is a database of managed objects accessed by network management protocols. It is a hierarchical collection of objects organized in a tree. To prevent naming conflicts, the Internet Assigned Numbers Authority (IANA) manages the structure and objects in the tree. While the top levels of the MIB are fixed, the IETF, equipment manufacturers, vendors and other organizations have defined specified sub-trees. Many managed devices also have "private" MIB extensions. These extensions make it possible to report additional information to a particular equipment manufacturer's proprietary management software or to other management software that is aware of the "private" MIB extensions. In 2002, the website "mibCentral" claimed that it indexes over 4,600 MIBs representing more than 630,000 MIB object definitions.

The Task Group has identified opportunities to enhance NRIC Best Practices in the area of software configuration change management and version control. There is also an opportunity to improve change management documentation, revision change history, and source material. In addition, there is a need for guidance in the area of software production standards affecting software configurations and software back-ups. Finally, there is an opportunity to enhance Best Practices in the area of manual and automated software configurations impacting installation and back-out procedures, change tools, upgrades, and limited/phased deployments.

**Test Environment Descriptions and Published Capacity**

The Task Group has identified opportunities to enhance NRIC Best Practices in the area of test environment descriptions along with the use of "published" capacity in software testing and qualification.

During the gap analysis, two areas were identified which require further investigation. The first area has to do with Software Warranty as it pertains to maintaining the integrity and security of outdated operating systems and network management software. Specifically, where networks may be operating software code that is not under a Service Level Agreement (SLA) with the equipment manufacturer. The second area spans Expert Systems/Knowledge Base Systems (a.k.a. pseudo Artificial Intelligence) and their possible affect on network reliability and interoperability. These systems consist of self-modifying code and may affect software qualification, operations, configuration management, and version control.

## 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.[44] 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 Learnings regarding the network reliability Best Practices from analysis of the industry survey:

- There is moderate to high risk to not 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[45]

A survey that focuses 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

[44]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

[45]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.

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 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.' "[46]**

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 Mangers

### 3.4.3.2 Network Types

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

- Cable
- Internet/Data
- Satellite
- Wireless

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

- Wireline

#### 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, NRIC V and NRIC VI 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)
= 1 for Disaster Recovery and Mutual Aid
= 3 for Mutual Aid
= 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 Public Data 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 Public Data Networks.

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

1. Engagement of over 60 industry subject matter experts (Section 2 and 3)
2. Articulation of over 70 attributes of Public Data Networks
3. Consideration of over 200 concerns regarding Public Data Networks
4. Formation of 8 Task Groups that provide systematic coverage of communications infrastructure elements (Section 3)
5. Identification of 11 gaps in existing NRIC Best Practices (Section 3)

The 11 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 Public Data Networks. Issue 3 of this report will identify existing Best Practices and recommend new Best Practices for Internet data services providers.

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 3B Document “Public Data 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).

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

ANSI - American National Standards Institute
ATIS – Alliance for Telecommunications Solutions
BITS - Financial Services Roundtable
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
GETS – Government Emergency Telecommunications Service
FCC – Federal Communications Commission
GETS – Government Emergency Telecommunications Service
HEMP – High Energy Modulated Pulse
IEC - International Engineering Consortium
IEEE - Institute of Electrical and Electronics Engineers
ISAC – Information Sharing and Analysis Center
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
PSPTNS – Packet Switched Public Telecommunications Network Services
SLA - Service Level Agreement
SME – Subject Matter Expert
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. NRIC VII Charter

## CHARTER
## of the
## NETWORK RELIABILITY and INTEROPERABILITY COUNCIL – VII

### A. The Committee's Official Designation

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

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

The purpose of the Council is to provide recommendations to the FCC and to the communications industry that, if implemented, shall under all reasonably foreseeable circumstances assure optimal reliability and interoperability of wireless, wireline, satellite, cable, and public data networks.[47] 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.[48] This means ensuring that

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

[48] 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).”

emergency communications networks are reliable, survivable and secure. It also means that emergency communications networks (including E911[49]) 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).

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.[50] 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

[49] “E911” is an acronym for Enhanced 911 service.
[50] The work of ESIF Study Group G will be considered in this effort.

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.

- 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. Public Data Network Attributes

***The following were proposed as PDN attributes during Focus Group discussions and do not represent consensus.***

**NETWORKS, STANDARD, OTHER**

- Historic PDN: X.25, SMDS
- Many Protocols
- Should describe PDN's on a functional basis
    - Do Not restricted PDNs to specific protocols (e.g., not just IP, ATM, SMDS)
    - PDN consist of:
        - PAN – Public Access Network - do not discriminate but may have access requirements (i.e. may restrict access)
            - Not totally open to the public
                - AOL is a PAN
            - Provides Subscriber Access to Major Backbones [A 'stub' network – overused term]
            - 'Edge' Network
        - (Pure) Transit Networks
            - Carries traffic from PANs
            - No Customer Access
        - Core' Network
- PDN have multiple personality disorder
    1) From consumer's perspective, the Internet (or PDAs) is a means to accessing content or services. Some of those services are communication tools, such as email and IM. Content is html based, streaming media or other sources. Another subset of content and services would include entertainment experiences, such as gaming.
    2) From the enterprise perspective, the Internet/PDAs is a connectivity tool, enabling communications between locations, clients, customers, etc. A huge component of this perspective includes a sales interface. Commerce portals and financial transactions are simply another storefront.
    3) The residual identity is comprised of research and other activities. However, only the above two components can be attributed to the growth and purpose that gives the Internet its life. In other words, we cannot have a discussion about the attributes of the Internet and yet ignore its identify.
- Internet, email services
    - Misconceptions: 'dial up' equals Internet
- Conglomeration of multiple physical layer platforms (ATM, Frame)
- Shared Network (vs. closed)
- Access Agnostic

**APPENDIX 5 (cont'd)**

- Multiple Physical Layers (transport):
  - Copper
  - Fiber
  - Wireless (e.g., WiFi)
  - Free Space Optics
- Security depends on both the public and private networks
- PDN can be characterized by the OSI reference model
  - Many items defined in Stack Layers
- Addressing Global Reachability
- Public
- Networks
- Data
- A 'Transmission Media' that is not application sensitive
- Service Characteristics
  - Performance, Security, Reachability, Network *Accessibility*
- Applications & Services that <u>often</u> attempt to fairly share resources
- Known address space vs. unknown address space
- Inter-carrier relationships are common
- Addressing with <u>Routing Mechanism</u> (BGP, other)
- Often under multiple administrative domains / authorities
- IP Address space is globally shared (assigned) – under RIR (Regional Internet Registry - addressing authorities)
- Internet applications are functionally dependent on DNS
- Uncertain Jurisdiction (global nature)
- Internet is Decentralized
- Often Any-to-Any
- Performance Characteristics
  - Today – driven by Market Demand
    - + Sal's /performance characteristics
    - + *Obsolete:* PDN are 'best effort'
  - 5 9's are 'port availability' are SLA driven
  - Latency, Loss, and Jitter are Network wide characteristics
  - Public Slaps are not the same as SLA

- Blurring of Reliability and Quality
- Connection-less (IP) and Connection-orientated
- Different <u>expectation</u> for different service applications
  - Phone vs. Email (gap is closing)
- Evolving
- Convergence
- Transition to an all digital & packet network
- Various/Different 'starting points'
- Trouble Shooting PDN
  - End User has visibility to global infrastructure (e.g., Ping/Trace Routes)
  - Requires secure management of network elements (e.g., SNMP data)

- Multiple administrative entities are often involved in problem resolution
    - Provider of the infrastructure
    - Customer facing trouble shooting
    - 3rd Party Partner (Peering, Data Center, Network-to-Network Interfaces)
    - On-Net / Off-Net
    - Provider of the connectivity to the Internet
    - (Possible end-user)

- High growth rate
    - Increasing demand
- Increasing Dependence of Public Safety, National Security, Financial Stability on PDNs
- Effective use of PDNs are a competitive advantage to individual corporations
    - Reduce cost of operations
    - Speed up delivery of new services
- Different statistical daily traffic patterns than PSTN
- Aggregate traffic profile is predictable (daily, monthly, yearly)
- Instantaneous real time statistical traffic patterns unpredictable (i.e. connectionless networks)
- Challenging for statistical abnormalities in traffic (i.e. connectionless networks)
- Any-to-Any characteristic of the PDN makes vulnerable to DDoS
    - Complicates traffic management
- Intelligence of the network is being pushed to the edge of the network
- Points of Infrastructure concentration (e.g., Telcom Hotels, Fiber right-a-ways)
- Property Managers play a key role in controlling the environment (e.g., power upgrades)
- Varying standards for building and network equipment
- Testing fail-over emergency and escalation plans are vital in light of rapid growth/change (e.g., evolving and upgrading power)

## PAYLOAD

- Internet is A Network of Networks (BGP is the existing mechanism)
- Often combine signaling and payload

## SOFTWARE

- Network Element software reliability is crucial
- SW upgrades require interoperability testing

## HARDWARE

- Increasing use of same hardware (integrated circuits) in the equipment
- Trend of outsourcing for HS/SW

**APPENDIX 5 (cont'd)**

## POWER

- Design with redundant power is relatively new
- Lack of data to monitor power outages (e.g., cable remotes)
- DC or AC power
- On-site end-user power is required to work
- End-user power may be regulated

## HUMAN

- Physical and cyber access to the control of the networks is not limited to few people (e.g., human error, malicious intent)
- Significant skill is required to design, configure, maintain, operate PDNs
- Increased trend to customer self service (i.e. automated self help)
- PDNs are highly ubiquitous?
- Wide variety of applications (voice, video, …)

**POLICY / REGULATORY ASPECTS Include:**

- Often unregulated
- Varied regulation
- Support for Critical/Essential Services
- No Universal Access Mandate
  - QoS of Applications
  - Undefined PDN Emergency Services
    - E911?
    - Legally required to provide?
  - VoIP
- Primary vs. Secondary Line Treatment/Priority
- Emerging Lawful Intercept Requirements (CALEA)
  - Expectations of User?
  -

**********

**Other Contributions**
**(Not PDN Attributes)**

- No fundamental security in PDN
- Security – corporate vs. public network and secure the network (all layers)
- "Internet Focus" (IP)
  - Below - Infrastructure
  - Above - Applications
- Focus on Layer 3 (not layers below)
- Internet requires BGP
- Mechanisms that encourage Private Address Space
- PDN reliability depends on upper layers for data integrity
- PDN is fundamentally an unreliable network
  - New Protocols address this
  - Reliability is enhanced above layer 3

# Appendix 6. Public Data Network Gaps

The 11 gaps identified by the PDN Focus Group are:

- **Environment Gap**

  **Managing Growth in Multi-Tenant Facilities**
  The Environment Task Group identified one gap in existing, documented NRIC Best Practices related to the complexity of managing growth in third party and multi-tenant environments (e.g., space, power, cooling).

- **Network Gaps**

  Four Network Gaps have been identified:

  **Network Design and Planning**
  73 Best Practices currently exist relative to network design. The Task Group has identified opportunities to enhance NRIC Best Practices in the following areas: the treatment of private address space, routing practice, and design audit.

  **Network Measurement and Management**
  One Best Practice exists relative to Equipment Suppliers measuring and improving quality. The Task Group has identified opportunities to expand and clarify the scope of the Best Practice to include Service Providers and Network Operators.

  **Network Spares Administration**
  At least 12 current Best Practices touch on spare equipment. The Task Group has identified an opportunity to improve guidance in the area of spares management.

  **Maintenance Window**
  One current Best Practice exists for the definition of maintenance windows. The Task Group has identified an opportunity to improve guidance in the communication of maintenance timeframes.

- **Power Gaps**

  **Proper Identification of Cables**
  Administration, maintenance and operations of network elements depend on proper identification of equipment. While there are numerous Best Practices that address administration, operations and maintenance, and while Network Operators currently employ various effective methods of cable labeling, the NRIC Best Practices do not document guidance in this area.

  **Back-Up Power for On-Premise Emerging Data Services Equipment**
  Emerging data services, such as Voice Over IP (VoIP) are increasingly viewed as critical services. As such, this equipment may need to continue to function even during commercial power outages. Because the end user equipment is

increasingly powered by local sources, back-up power consideration should be explored. As these networks are still very new, further analysis is pending.

- **Software Gaps**

**Management Information Base (MIB)**

Due to the quantity and interactions of "private" MIB extensions with proprietary and other management software, the Task Group has identified opportunities to enhance NRIC Best Practices in the areas of MIB support, standardization, and documentation. In addition, there is opportunity to improve support of environmental variables in MIBs.

**Crash Diagnostic Memory**

The Task Group has identified opportunities to enhance NRIC Best Practices in the area of crash diagnostic memory storage and the use non-volatile memory. There is added opportunity to improve storage of core dumps and system states associated with a crash.

**Software Configuration**

The Task Group has identified opportunities to enhance NRIC Best Practices in the area of software configuration change management and version control. There is also an opportunity to improve change management documentation, revision change history, and source material. In addition, there is a need for guidance in the area of software production standards affecting software configurations and software back-ups. Finally, there is an opportunity to enhance Best Practices in the area of manual and automated software configurations impacting installation and back-out procedures, change tools, upgrades, and limited/phased deployments.

**Test Environment Descriptions and Published Capacity**

The Task Group has identified opportunities to enhance NRIC Best Practices in the area of test environment descriptions along with the use of "published" capacity in software testing and qualification.

# 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 Public Data 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.