Network Reliability and Interoperability Council (NRIC)

Year 2000: Ushering in the New Millennium

February, 2001

Table of Contents

1. Executive Summary

This report details the efforts of the telecommunications industry to prepare for one of the greatest challenges it has ever faced – the rollover to the Year 2000. The unprecedented levels of networking, cooperation, teamwork, and information sharing unleashed through the Network Reliability and Interoperability Council (NRIC) along with the leadership and involvement of the FCC enabled our industry to experience a smooth and seamless transition into the 21st century.

The contents of this report provide some background on the challenges posed by the Y2K event and describe the role played by NRIC in successfully meeting these challenges. Toward that end, the report contains the assessments of the various NRIC IV Focus Groups regarding our industry's readiness for this unique event and highlights the actual transition into Year 2000. Finally, the report captures the key lessons learned from the Y2K experience that can be carried forward and leveraged in future challenging opportunities.

2. Year 2000 Challenge

The Year 2000 problem resulted from a convention initially used by computer programmers starting back in the 1960s to store dates in software using only two digits for the year, thus reducing the need for scarce and expensive computer memory. Therefore, 1972 was represented in the code as "72". As a result, computers, software, and microchips using a two-digit year, unless otherwise corrected, may have interpreted "00" as the year 1900 rather than the year 2000. The misinterpretation of a date as 1900 instead of 2000 could have caused computers and digital systems to perform incorrectly or stop working altogether.

While programmers were cognizant of the fact that this memory-saving convention would not work post-1999, they erroneously assumed that that the software being written would become obsolete and be replaced well before the turn of the century. In many cases, this turned out to simply not be the case.

Furthermore, there was some concern about how computers would behave on Leap Day in the Year 2000. This stemmed from the fact that most years divisible by 100 are not leap years. However, any year divisible by 400 does have an extra day added, making 2000 a leap year. Unless programmers accounted for this in their coding, programs may have produced erroneous results on Leap Day in 2000.

While the ubiquitous nature of the Year 2000 issue impacted all industries, the challenge was particularly daunting in telecommunications. The "network" is large and complex and is owned and operated by many different companies. A call typically often travels over many different parts of the network while being completed and sometimes employs a variety of technologies (e.g. wireline, wireless, satellite services). And finally, adding to the challenge was the fact that the telephone network is one of the most critical infrastructures that could have been affected by the Year 2000 transition in that it impacts the manner in which people around the world communicate with each other.

3. NRIC Background

The Network Reliability and Interoperability Council (NRIC) is the successor to the Network Reliability Council (NRC) that was initially organized by the FCC in January of 1992. The Council brings together leaders of the telecommunications industry and telecommunications experts from academic, consumer, and other organizations to explore and recommend measures that will enhance network reliability and interoperability.

The charter of the first Council (NRC I) was to analyze the causes of service outages in various local exchange and inter-exchange wireline telephone networks and to develop recommendations to reduce the number and effects of outages on consumers. The Council's analysis and nearly 300 recommendations were provided to the Commission and published in *Network Reliability: A Report to the Nation* and can be accessed electronically at www.nric.org/pubs/nric1.

The second Council (NRC II) was re-charted in 1994 to address regional / demographic variations of network reliability, network interconnection, changing technologies, and essential communications / telecommuting capabilities during emergencies. NRC II's findings were detailed in its February, 1996 report, *Network Reliability – The Path Forward* and can be accessed electronically at www.nric.org/pubs/nric2.

The third Council (NRIC III) charter was revised, and its title changed to the present "Network Reliability and Interoperability Council," by the FCC in April, 1996 to advise the Commission on the implementation of Section 256 of the *Telecommunications Act*, to provide recommendations for both the FCC and the telecommunications industry to assure optimal reliability and interoperability of, and accessibility and interconnectivity to, public telecommunications networks, to advise on how the Commission most efficiently could conduct oversight of coordinated telecommunications network planning, and to assess the Commission's role in the development of telecommunications standards. NRIC III's report, *NRIC Network Interoperability – The Key to Competition* was presented to the Commission in July of 1997 and can be accessed electronically at www.nric.org/pubs/nric3/reportj9.doc.

In July of 1998, the Commission announced the appointment of AT&T Chairman and CEO C. Michael Armstrong as Chairman of NRIC IV. Under its amended charter, the Council was asked to advise the FCC on the efforts of the telecommunications industry to prepare for the Year 2000 conversion with the goal of assuring optimal reliability, interoperability, and interconnectivity of, and accessibility to, the public telecommunications networks.

Specifically, the Council was asked to assess the magnitude of Year 2000 risks and review efforts taken to reduce those risks, and determine what additional steps should be taken to further mitigate risks. To perform the necessary analysis and develop appropriate recommendations, NRIC IV formed 3 focus groups to assess the following issues contained within its charter:

- Focus Group 1 – What is the impact of the "Year 2000 problem" on public telecommunications networks and services?
- Focus Group 2 – What is the impact of the "Year 2000 problem" on access to the telecommunications networks and services (i.e. CPE perspective)?
- Focus Group 3 – What is the current status of network reliability?

In addition, a steering committee was established to set the agendas for meetings, review the progress of the Focus Groups, resolve Focus Group and cross-group issues, formulate policies, and oversee the administrative fund.

Within Focus Group 1, 3 subcommittees were formed to assess:

- Y2K readiness of telecommunications networks
- Y2K testing performed on networks
- Y2K contingency plans for networks to further mitigate risks during the transition

Focus Group 2 was comprised of 2 subcommittees addressing the following issues:

- Y2K readiness and testing of CPE
- Y2K contingency planning for CPE

Similarly, Focus Group 3 consisted of 2 subcommittees to examine the following areas:

- Industry best practices review to determine whether these practices should be modified or supplemented
- Data analysis and future considerations

See Appendix A of this report for a listing of companies / organizations involved with carrying out the charter of NRIC IV.

Following NRIC IV, the fifth Council (NRIC V) was re-chartered to provide recommendations to the FCC and to the telecommunications industry that, when implemented, will assure optimal reliability and interoperability of public telecommunications networks. NRIC V is focusing on the following areas:

- Review of work relating to the Year 2000 transition
- Network reliability
- Wireline network special integrity

- Interoperability

4. NRIC IV Assessment of Y2K Industry Readiness

The final assessment of NRIC IV's Focus Group 1 regarding the readiness, testing and contingency plans for the public telecommunications networks for the Year 2000 transition was delivered on October 14, 1999. At that time, it was reported that the major domestic telecommunications carriers (both LECS and IXCs) were complete with their remediation and implementation programs whereas most mid / small size LECs (approximately 98%) were targeted to be compliant by December of 1999. On the international front, the risk profile of traffic to / from the United States continued to improve but nevertheless posed some degree of concern particularly from low volume traffic countries.

In terms of Y2K testing of the networks, it was reported that no significant gaps in interoperability testing had been identified with testing coverage spanning the majority of access and IXC switch and signaling vendors. No Y2K anomalies in any completed testing program had been identified.

To support the collection of industry status information during the Year 2000 rollover, the NCC/NCS was established as the focal point for this effort with participation from major LECS, IXCs, Industry Forums, International Telecommunications Union (ITU) members, and government agencies. Information collected by the NCC would be shared with the FCC and the Information Coordination Center (ICC).

Based on these findings, it was felt that the risk of failure of the domestic telecommunications network was minimal. Likewise, the risk of international call failure between North America and other regions of the world was also perceived to be minimal; however, potential impacts related to the Year 2000 transition could include call setup delay due to network congestion in foreign networks, degradation of service quality over time due to non-compliant components in foreign networks, and unpredictable infrastructure (e.g. energy) failures in some foreign countries.

The entire report of NRIC IV's Focus Group 1 can be found under Appendix B of this report.

NRIC IV's Focus Group 2, which concentrated its analysis on Y2K issues pertaining to access to telecommunications networks and services (i.e. CPE) reported that some telecommunications devices (e.g. Public Safety Answering Positions, or PSAPs) were more likely to be impacted by the Year 2000 event than others (e.g. facsimile machines). In general, it was felt that CPE was not likely to experience 'critical' problems provided that users prepared properly by inventorying their equipment, contacting vendors to ascertain Y2K status, testing (if possible) and replacing if necessary.

An overview report issued by Focus Group 2, subcommittee 1 can be found under Appendix C of this report. The entire set of reports issued by this subcommittee including Y2K readiness / testing evaluations of various types of CPE (e.g. PBXs, modems, cellular devices, etc.) can be accessed electronically at www.nric.org/fg/fg2/index.html.

Subcommittee 2 under Focus Group 2 evaluated contingency planning issues pertaining to CPE and issued the report found under Appendix D. In short, the subcommittee concluded that given the diverse nature of most types of CPE (i.e. large quantities deployed, numerous suppliers, etc.) the responsibility for contingency planning rested solidly with the end user / owner of the CPE. The subcommittee also provided a series of recommendations to the FCC, CPE manufacturers, CPE based service providers, and CPE end users focused toward ensuring that the CPE end user was appropriately prepared for typical Y2K situations that could arise.

With respect to work performed by Focus Group 3, NRIC, with input from the Alliance for Telecommunications Industry Solutions' (ATIS) Network Reliability Steering Committee (NRSC), reported on outage incidents across the telecommunications network. The report stated most failure categories were within control limits but that outage exceptions were found in power, digital cross connect systems and those for which the root cause was procedural errors. The NRIC report pointed out that the industry is addressing these exceptions through recently published NRSC Procedural Errors recommendations (www.atis.org) and through "Power" best practices from NRIC's Focus Group 3's Best Practices subcommittee.

In addition, the Data Analysis and Future Considerations subcommittee developed guidelines and templates designed to remove ambiguities and improve the quality of telecommunications outage reporting.

The reports issued by the Network Reliability and Data Analysis / Future Considerations subcommittees under Focus Group 3 can be found under Appendices E and F of this report, respectively.

Based upon the extensive analysis of NRIC IV, it was widely perceived that the U.S. telecommunications industry was indeed well prepared for the Year 2000 event. A press release detailing this assessment was issued on November 9, 1999 and can be found under Appendix G of this report.

5. Highlights of the Year 2000 Transition

Despite the favorable assessments of Y2K readiness among experts within the telecommunications industry and other industries at large, the world waited anxiously as the next century was ushered in from time zone to time zone around the globe. Within the telecommunications industry, the typical scenario resulted in higher call volumes and traffic spikes as the Year 2000 arrived with a return to "normal" call volumes within one hour. Despite these brief periods of heavy congestion on the network during the transition, calls continued to complete with very few Y2K-related incidents experienced. Problems that were reported had virtually no impact on customers.

This favorable outcome was also experienced by other industry sectors including finance, power, and transportation along with federal, state, and local government agencies. In short, no major problems were reported.

This same pattern held true for the Leap Year transition with only minor glitches being reported.

This is not to suggest that there weren't some bumps along the way. For example…

- A Y2K computer problem temporarily blinded several orbiting U.S spy satellites for several hours
- A Y2K-related bug affected a Federal Aviation Administration system used to dispatch weather information to pilots and was quickly remedied
- Seven nuclear power plants around the country reported minor problems with computer systems that did not affect plant safety in any way
- Amtrak reported difficulties identifying the trains on its tracks at its Philadelphia Control Center – the problem was promptly fixed without disrupting travel
- A security system failed at a Bureau of Alcohol, Tobacco and Firearms office
- Approximately 1,200 ATMs in Japanese Post Offices shut down due to computer problems
- Computers at western Japanese weather stations reported heavy rainfall despite clear skies
- Japan's Ministry of Posts and Telecommunications (MPT) reported a handful of Y2K-related problems that were quickly resolved with minimal impact to the public
- Japan also reported computer problems with 3 nuclear power plants
- A glitch affected a program in a French defense satellite

Source: Various *CNN* newswire articles

Furthermore, Y2K bugs are still being identified a full year after the crossover to the 21st century. These recent incidents indicate that concern for Y2K problems must still continue.

- 7-Eleven Inc. reported a Y2K-like glitch beginning January 1, 2001 when cash registers at its stores identified the date as January 1, 1901 instead of the correct one. This problem temporarily left the company's main systems unable to process credit card transactions.

Source: *COMPUTERWORLD* newswire article

- Norway's national railway system experienced Y2K-related problems in the morning of December 31st, 2000 that rendered several airport express trains and high-speed long-distance trains temporarily inoperable.

  Source: *The Associated Press* newswire article

6. NRIC V Post-Year 2000 Survey

In July, 2000 a post-Year 2000 survey was sent to NRIC V members with reminder notices distributed in August. The cover letter for the survey and the survey form can be found under Appendices H and I, respectively, of this report.

The purpose of the survey was to gather data to allow for a final review of the Y2K transition and determine:

- What happened during the rollover?
- What is being done to maintain the gains afforded by Year 2000?
- What were the key learnings of this event?

The survey results revealed that the number and duration of Y2K-related incidents was minimal with the impact on customers being insignificant in virtually all cases. Where Y2K-related problems were found, they tended to impact business processes such as billing and provisioning and not call processing. Also of importance was the fact that regression testing has been routinely incorporated into current processes to ensure that Y2K-compliant code is not inadvertently broken in the future.

7. Lessons Learned

The Year 2000 experience certainly provided some unique learning opportunities that can be leveraged to more effectively deal with future challenging programs. A partial list of these lessons includes the following:

- Program management…program management…program management is critical in managing such a challenging project
- NRIC was an indispensable forum for sharing experiences and leveraging knowledge and strategies
- Centralized coordination and control resulting in common standards, tools, and certifications balanced with distributed execution are keys to success
- Interdependencies within and between industries are far more common than ever imagined
- A non-traditional approach is required to achieve better than traditional results

- Establish principles and policies that support teamwork and mission accomplishment
- Objective scorecards / dashboards are essential to evaluate ongoing progress
- Ongoing need exists for continued testing and independent validation and verification (IV&V) programs
- Interoperability testing is invaluable to demonstrate end-to-end performance
- Telecommunications networks are complex, extensive in scope, and quite robust
- External / internal two-way communications are mandatory
- Business continuity (i.e. contingency planning) is critical
- Involve all stakeholders as early in the process as possible
- Instill a sense of urgency and empower team members
- Triage requirements for best results – concentrate on mission critical issues first

Other benefits companies realized as a result of Y2K include at least some of the following:

- Up-to-date and accurate inventories
- Better control over IT technologies
- Improved communications with partners and suppliers
- Accelerated retirement of old applications / systems and components
- Upgrades to the latest releases for IT and network platforms
- Improvements in software quality, productivity process and practices, and testing
- Better appreciation of the effectiveness of software tools in maintenance and testing
- Data security improvements
- Enhanced business continuity plans

Despite the occasional glitches still being reported with Y2K, it is tough to argue that the rollover to the 21st century has been anything but successful. The fact that the Y2K transition turned out to be such a "non-event" has even led some people to wonder if Y2K precautions undertaken were excessive. So what were some of the underlying factors that resulted in the Y2K rollover being so uneventful? These include:

- Potential Y2K problems were indeed fixed
- Some of the potential Y2K problems were exaggerated
- Many potentially faulty systems were turned off for New Year's or run manually
- Some systems had a lower load, and many systems had a higher degree of support, than normal
- Some Y2K bugs have not become visible yet
- Some problems have been de-emphasized, ignored or not reported

- Some of the problems occurred in Third World countries that were less dependent on computer technology and more accustomed to disruptions

Source: *Cutter IT Journal, July 2000*

8. Summary

Through the impressive leadership, representation and involvement by NRIC member groups and the FCC, the transition into the 21st century has been relatively uneventful. The occasional Y2K-related glitches notwithstanding, the telecommunications networks have continued to perform to its normal high standards with almost unfailing regularity.

Despite this successful crossover into the Year 2000 and beyond, the focus on Y2K must continue. An ongoing need exists to incorporate Y2K work within the framework of "business as usual" with a focus on:

- "Windowing" awareness and maintenance
- Regression testing to ensure that Y2K-remediated code remains compliant in the future
- Continued monitoring and evaluation of Y2K-related incidents

Undoubtedly, had the Y2K challenge been left unaddressed it would have significantly disrupted everyday life in many parts of the world. Ironically, because the challenges inherent in Y2K were managed so successfully, the full extent of the threat it posed to everyday life will never be known. It is a testimony to the individuals within NRIC, the FCC, and a cast of thousands throughout this industry and others whose leadership, dedication, and tireless efforts helped avert the crisis.

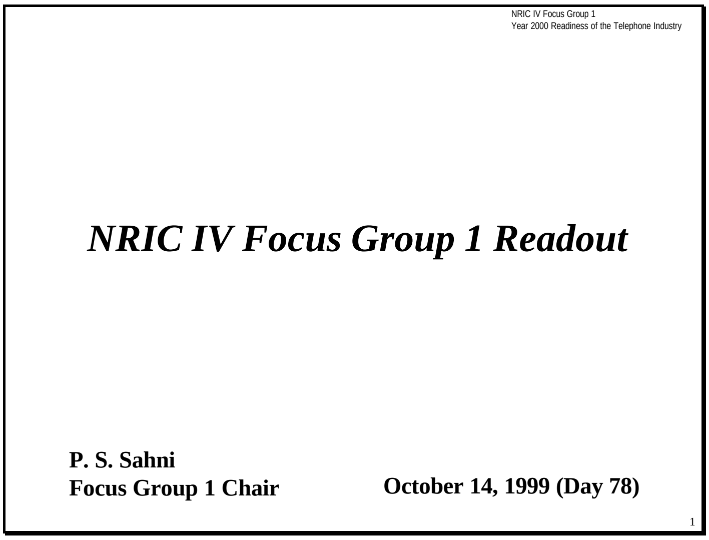
9. Appendices

Appendix A: NRIC IV Company / Organization Membership List

- 3Com Corporation
- AFL-CIO
- Alliance for Public Technology
- Alliance for Telecommunications Industry Solutions
- Alpha Lyracom / PanAm Satellite
- America Online, Inc.
- Ameritech
- Association for Local Telecommunications Services
- AT&T Corp.
- Bell Atlantic
- BellSouth Corporation
- The Boeing Company
- Cable Telecommunications Association
- Cable Television Laboratories, Inc.
- Cellular Telecommunications Industry Association
- CISCO
- Communications Workers of America
- Competitive Telecommunications Association
- COMSAT Corporation
- Cox Communications
- Frontier
- GTE Corporation
- Hughes Electronics Corporation
- International Communications Association
- Information Technology & Telecommunications Association
- Information Technology Industry Council
- Lucent Technologoies
- Matsushita (Panasonic)
- McLeod
- MCI Communications Corp.
- Motorola, Inc.
- National Association of Regulatory Utility Commissions
- National Association of State Utility Consumer Advocates
- National Cable Television Association
- National Communications Systems
- National Telecommunications and Information Administration
- Newbridge Networks
- NextWave Telecom, Inc.
- Nortel Networks
- The Organization for the Promotion and Advancement of Small Telecommunications Companies
- Office of Science and Technology Policies
- Personal Communications Industry Association
- SBC Communications, Inc.
- Sprint
- Telco Year 2000 Forum
- Telcordia
- Telecommunications Industry Association
- Time Warner Cable
- US West Communications
- United States Telephone Association

Appendix B: NRIC IV Focus Group 1 Final Readout

Slide 1



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

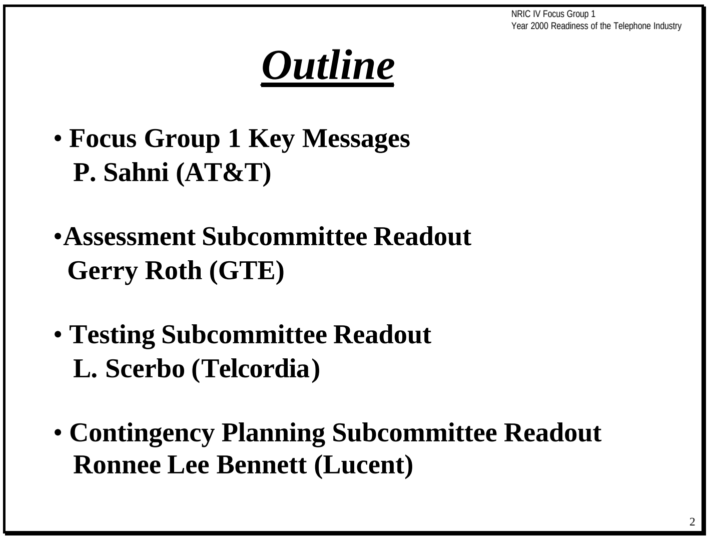
NRIC IV Focus Group 1 Readout

P. S. Sahni
Focus Group 1 Chair

October 14, 1999 (Day 78)

1

Slide 2



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Outline

- **Focus Group 1 Key Messages**
  P. Sahni (AT&T)

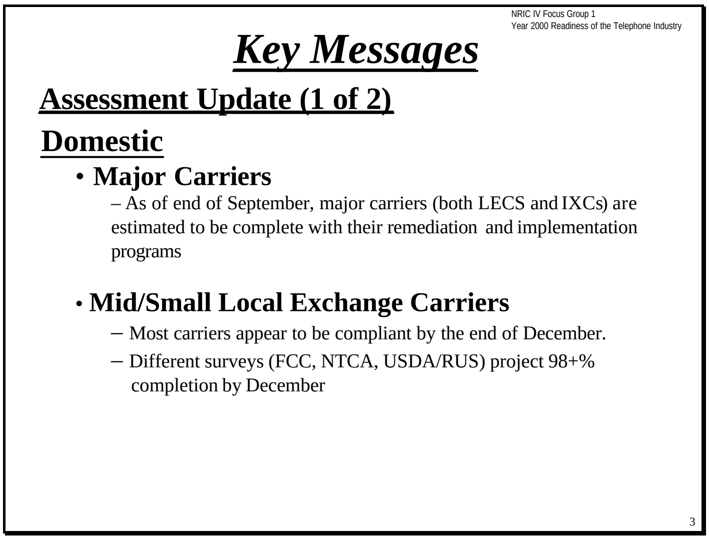
- **Assessment Subcommittee Readout**
  Gerry Roth (GTE)

- **Testing Subcommittee Readout**
  L. Scerbo (Telcordia)

- **Contingency Planning Subcommittee Readout**
  Ronnee Lee Bennett (Lucent)

2

Slide 3



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

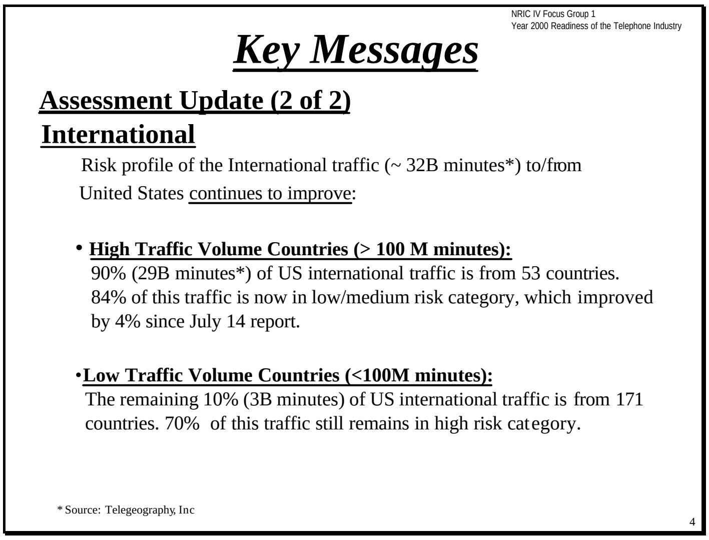
Key Messages

Assessment Update (1 of 2)

Domestic

- **Major Carriers**
  - As of end of September, major carriers (both LECS and IXCs) are estimated to be complete with their remediation and implementation programs
- **Mid/Small Local Exchange Carriers**
  - Most carriers appear to be compliant by the end of December.
  - Different surveys (FCC, NTCA, USDA/RUS) project 98+% completion by December

Slide 4



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Key Messages

Assessment Update (2 of 2)

International

Risk profile of the International traffic (~ 32B minutes*) to/from United States continues to improve:

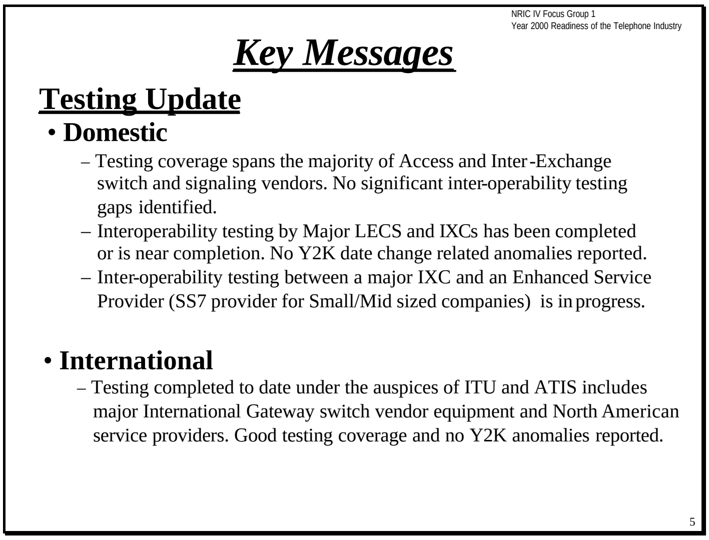
- **High Traffic Volume Countries (> 100 M minutes):** 90% (29B minutes*) of US international traffic is from 53 countries. 84% of this traffic is now in low/medium risk category, which improved by 4% since July 14 report.

- **Low Traffic Volume Countries (<100M minutes):** The remaining 10% (3B minutes) of US international traffic is from 171 countries. 70% of this traffic still remains in high risk category.

* Source: Telegeography, Inc

4

Slide 5



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Key Messages

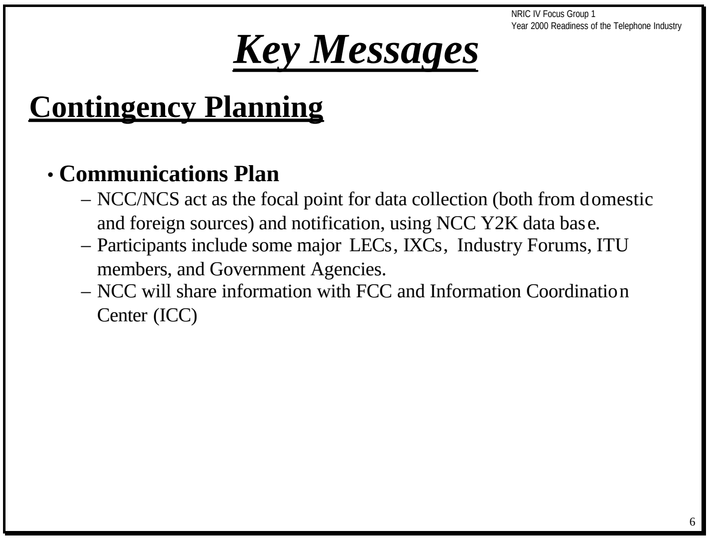
Testing Update

- **Domestic**
  - Testing coverage spans the majority of Access and Inter-Exchange switch and signaling vendors. No significant inter-operability testing gaps identified.
  - Interoperability testing by Major LECS and IXCs has been completed or is near completion. No Y2K date change related anomalies reported.
  - Inter-operability testing between a major IXC and an Enhanced Service Provider (SS7 provider for Small/Mid sized companies) is in progress.

- **International**
  - Testing completed to date under the auspices of ITU and ATIS includes major International Gateway switch vendor equipment and North American service providers. Good testing coverage and no Y2K anomalies reported.

5

Slide 6



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

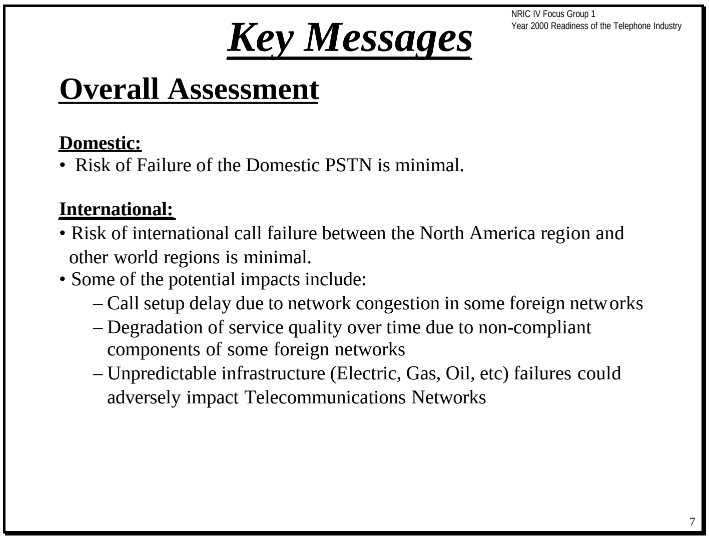
Key Messages

Contingency Planning

- **Communications Plan**
  - NCC/NCS act as the focal point for data collection (both from domestic and foreign sources) and notification, using NCC Y2K data base.
  - Participants include some major LECs, IXCs, Industry Forums, ITU members, and Government Agencies.
  - NCC will share information with FCC and Information Coordination Center (ICC)

6

Slide 7



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Key Messages

Overall Assessment

Domestic:

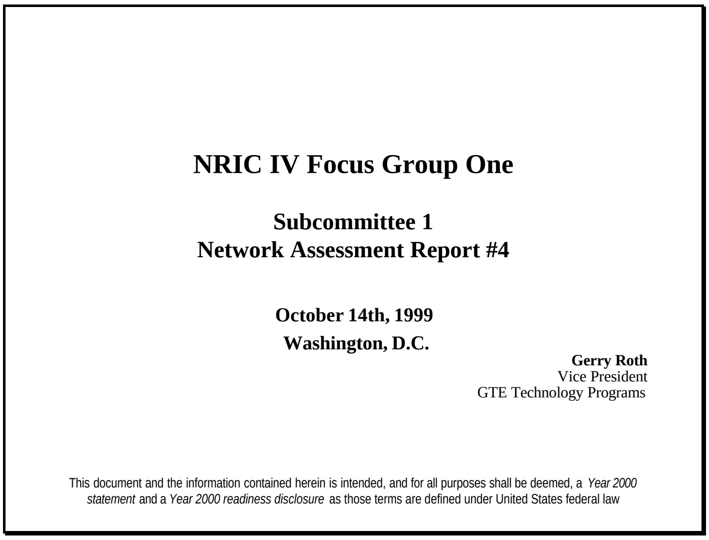
- Risk of Failure of the Domestic PSTN is minimal.

International:

- Risk of international call failure between the North America region and other world regions is minimal.
- Some of the potential impacts include:
  - Call setup delay due to network congestion in some foreign networks
  - Degradation of service quality over time due to non-compliant components of some foreign networks
  - Unpredictable infrastructure (Electric, Gas, Oil, etc) failures could adversely impact Telecommunications Networks

7

Slide 8



NRIC IV Focus Group One

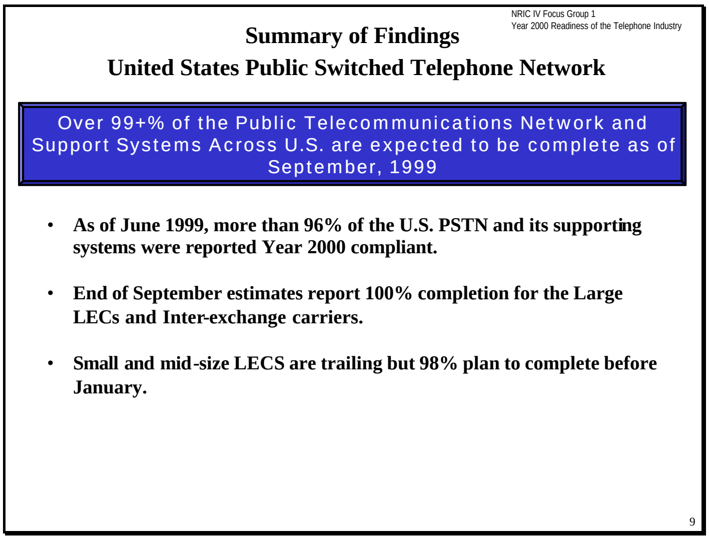
Subcommittee 1
Network Assessment Report #4

October 14th, 1999
Washington, D.C.

Gerry Roth
Vice President
GTE Technology Programs

This document and the information contained herein is intended, and for all purposes shall be deemed, a *Year 2000 statement* and a *Year 2000 readiness disclosure* as those terms are defined under United States federal law

Slide 9



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

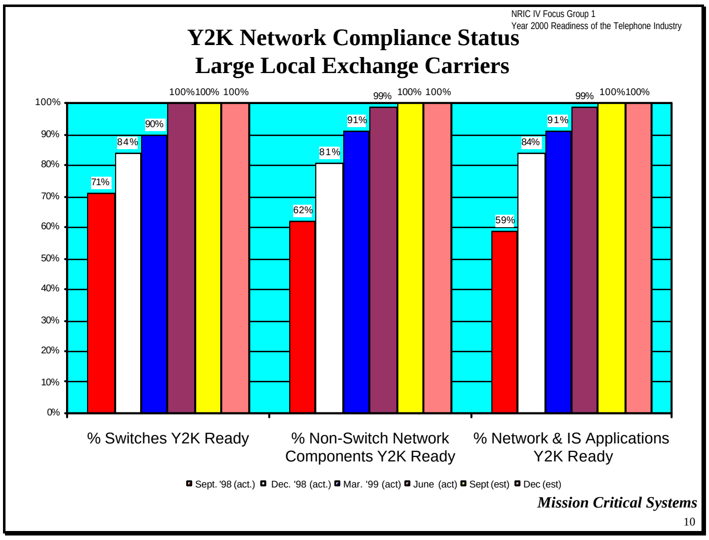
Summary of Findings
United States Public Switched Telephone Network

Over 99+% of the Public Telecommunications Network and Support Systems Across U.S. are expected to be complete as of September, 1999

- **As of June 1999, more than 96% of the U.S. PSTN and its supporting systems were reported Year 2000 compliant.**
- **End of September estimates report 100% completion for the Large LECs and Inter-exchange carriers.**
- **Small and mid-size LECS are trailing but 98% plan to complete before January.**

9

Slide 10



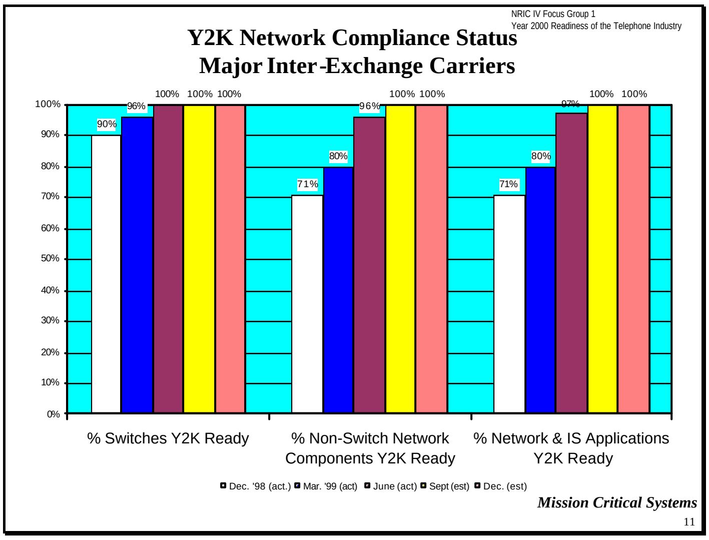
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Network Compliance Status
Large Local Exchange Carriers

Mission Critical Systems

10

Slide 11



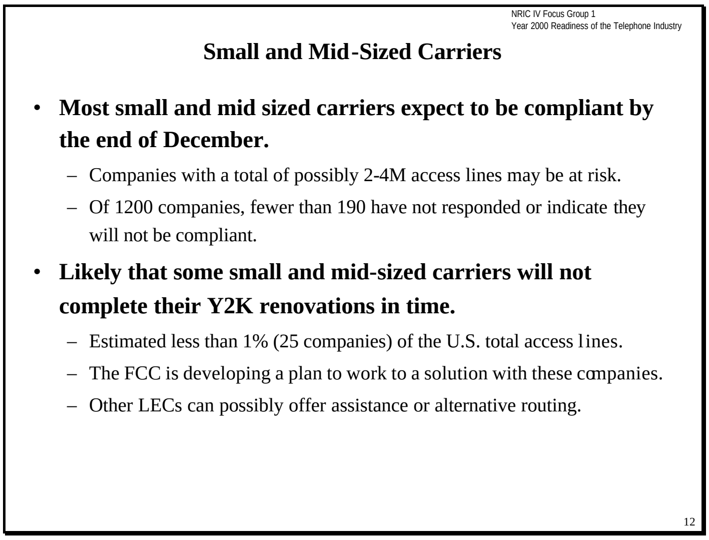
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Network Compliance Status
Major Inter-Exchange Carriers

Mission Critical Systems

11

Slide 12



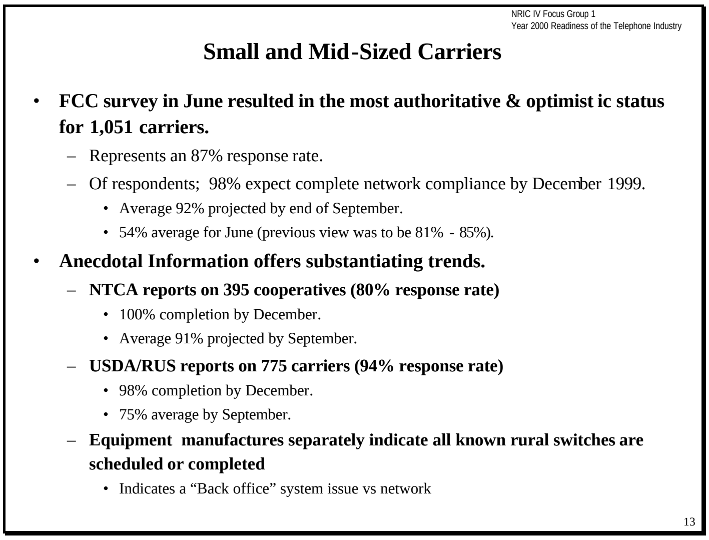
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Small and Mid-Sized Carriers

- **Most small and mid sized carriers expect to be compliant by the end of December.**
  - Companies with a total of possibly 2-4M access lines may be at risk.
  - Of 1200 companies, fewer than 190 have not responded or indicate they will not be compliant.
- **Likely that some small and mid-sized carriers will not complete their Y2K renovations in time.**
  - Estimated less than 1% (25 companies) of the U.S. total access lines.
  - The FCC is developing a plan to work to a solution with these companies.
  - Other LECs can possibly offer assistance or alternative routing.

12

Slide 13



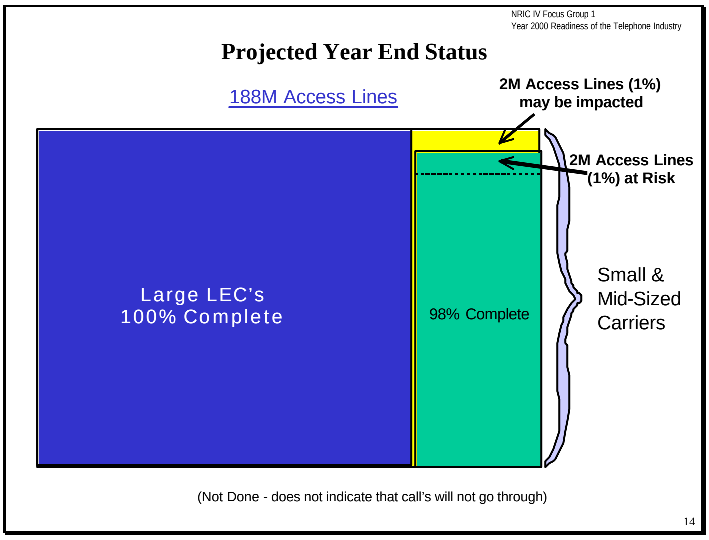
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Small and Mid-Sized Carriers

- **FCC survey in June resulted in the most authoritative & optimist ic status for 1,051 carriers.**
  - Represents an 87% response rate.
  - Of respondents; 98% expect complete network compliance by December 1999.
    - Average 92% projected by end of September.
    - 54% average for June (previous view was to be 81% - 85%).
- **Anecdotal Information offers substantiating trends.**
  - **NTCA reports on 395 cooperatives (80% response rate)**
    - 100% completion by December.
    - Average 91% projected by September.
  - **USDA/RUS reports on 775 carriers (94% response rate)**
    - 98% completion by December.
    - 75% average by September.
  - **Equipment manufactures separately indicate all known rural switches are scheduled or completed**
    - Indicates a “Back office” system issue vs network

13

Slide 14



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Projected Year End Status

188M Access Lines

2M Access Lines (1%) may be impacted

2M Access Lines (1%) at Risk

Large LEC's
100% Complete

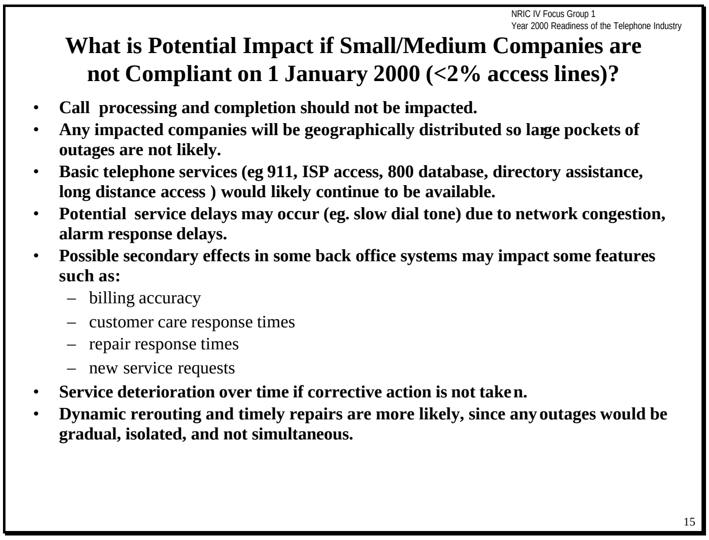
98% Complete

Small &
Mid-Sized
Carriers

(Not Done - does not indicate that call's will not go through)

14

Slide 15



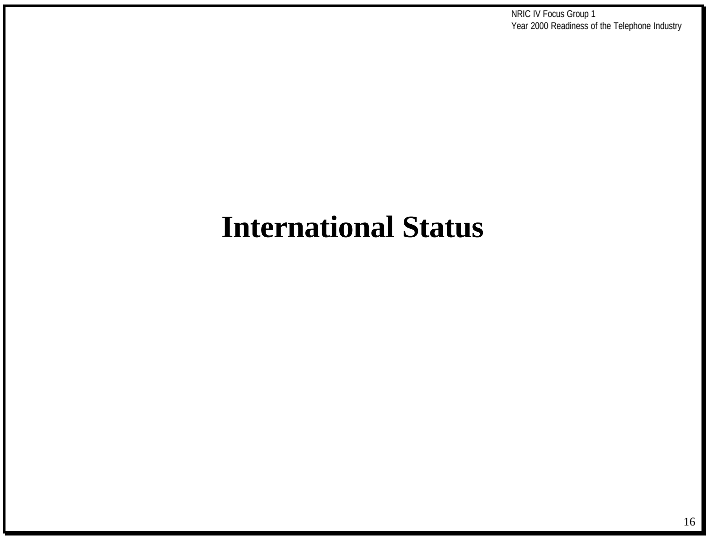
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

What is Potential Impact if Small/Medium Companies are not Compliant on 1 January 2000 (<2% access lines)?

- **Call processing and completion should not be impacted.**
- **Any impacted companies will be geographically distributed so large pockets of outages are not likely.**
- **Basic telephone services (eg 911, ISP access, 800 database, directory assistance, long distance access) would likely continue to be available.**
- **Potential service delays may occur (eg. slow dial tone) due to network congestion, alarm response delays.**
- **Possible secondary effects in some back office systems may impact some features such as:**
  - billing accuracy
  - customer care response times
  - repair response times
  - new service requests
- **Service deterioration over time if corrective action is not taken.**
- **Dynamic rerouting and timely repairs are more likely, since any outages would be gradual, isolated, and not simultaneous.**

15

Slide 16

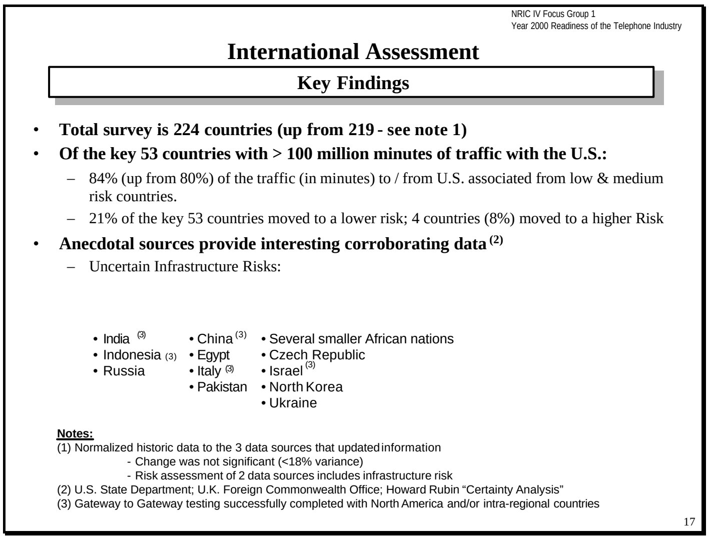


NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

International Status

16

Slide 17



International Assessment

Key Findings

- **Total survey is 224 countries (up from 219 - see note 1)**
- **Of the key 53 countries with > 100 million minutes of traffic with the U.S.:**
  - 84% (up from 80%) of the traffic (in minutes) to / from U.S. associated from low & medium risk countries.
  - 21% of the key 53 countries moved to a lower risk; 4 countries (8%) moved to a higher Risk
- **Anecdotal sources provide interesting corroborating data [2]**
  - Uncertain Infrastructure Risks:

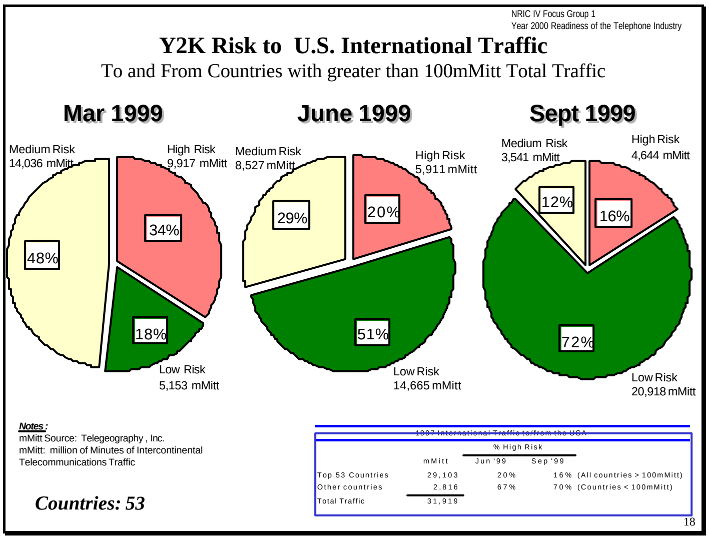
- India [3]
- Indonesia [3]
- Russia

- China [3]
- Egypt
- Italy [3]
- Pakistan

- Several smaller African nations
- Czech Republic
- Israel [3]
- North Korea
- Ukraine

Notes:
(1) Normalized historic data to the 3 data sources that updated information
- Change was not significant (<18% variance)
- Risk assessment of 2 data sources includes infrastructure risk
(2) U.S. State Department; U.K. Foreign Commonwealth Office; Howard Rubin "Certainty Analysis"
(3) Gateway to Gateway testing successfully completed with North America and/or intra-regional countries

Slide 18



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Risk to U.S. International Traffic

To and From Countries with greater than 100mMitt Total Traffic

Notes :
mMitt Source: Telegeography , Inc.
mMitt: million of Minutes of Intercontinental Telecommunications Traffic

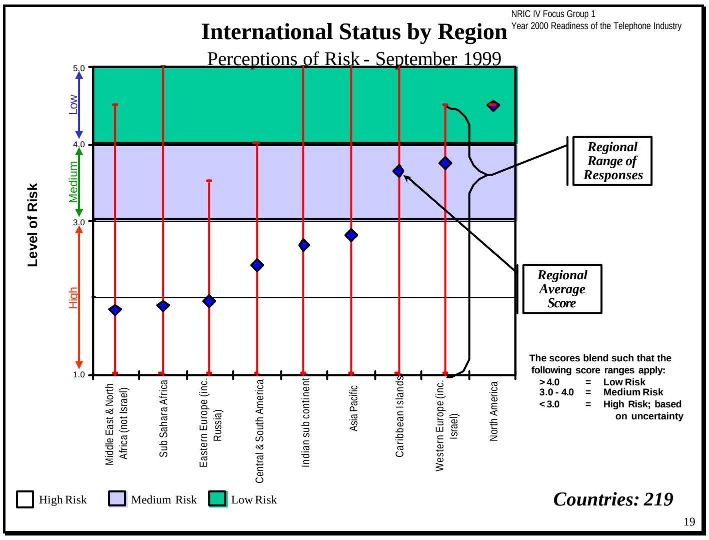
Countries: 53

1997 International Traffic to/from the USA

		% High Risk		
	mMitt	Jun '99	Sep '99	
Top 53 Countries	29,103	20%	16%	(All countries > 100mMitt)
Other countries	2,816	67%	70%	(Countries < 100mMitt)
Total Traffic	31,919			

18

Slide 19



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

International Status by Region

Perceptions of Risk - September 1999

Regional Range of Responses

Regional Average Score

The scores blend such that the following score ranges apply:

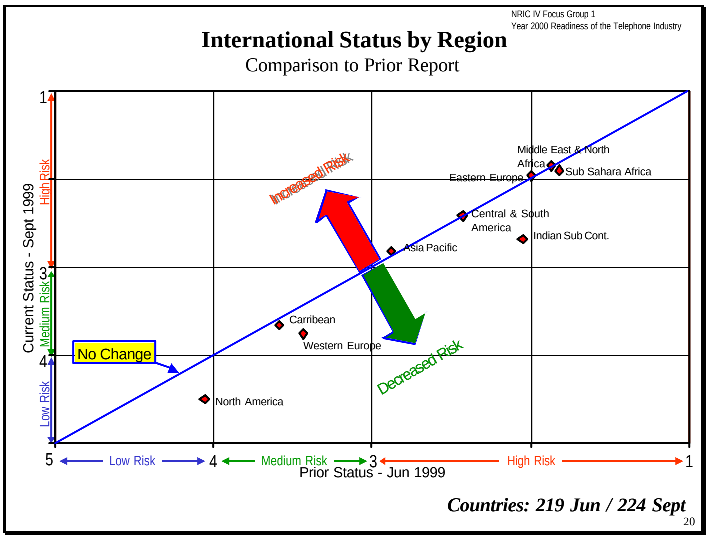
> 4.0	=	Low Risk
3.0 - 4.0	=	Medium Risk
< 3.0	=	High Risk; based on uncertainty

□ High Risk ▨ Medium Risk 🟩 Low Risk

Countries: 219

19

Slide 20



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

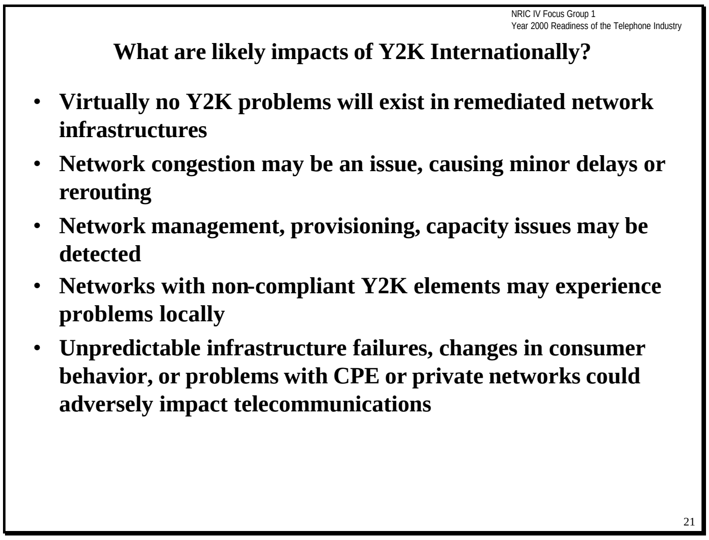
International Status by Region

Comparison to Prior Report

Countries: 219 Jun / 224 Sept

20

Slide 21



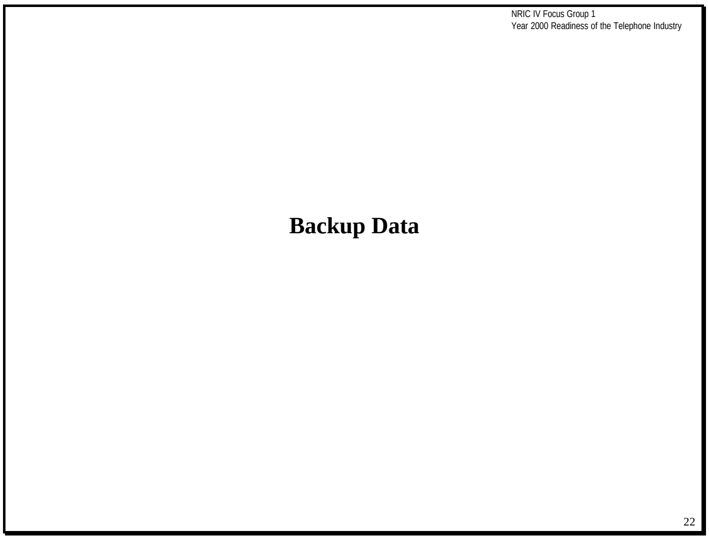
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

What are likely impacts of Y2K Internationally?

- **Virtually no Y2K problems will exist in remediated network infrastructures**
- **Network congestion may be an issue, causing minor delays or rerouting**
- **Network management, provisioning, capacity issues may be detected**
- **Networks with non-compliant Y2K elements may experience problems locally**
- **Unpredictable infrastructure failures, changes in consumer behavior, or problems with CPE or private networks could adversely impact telecommunications**

21

Slide 22

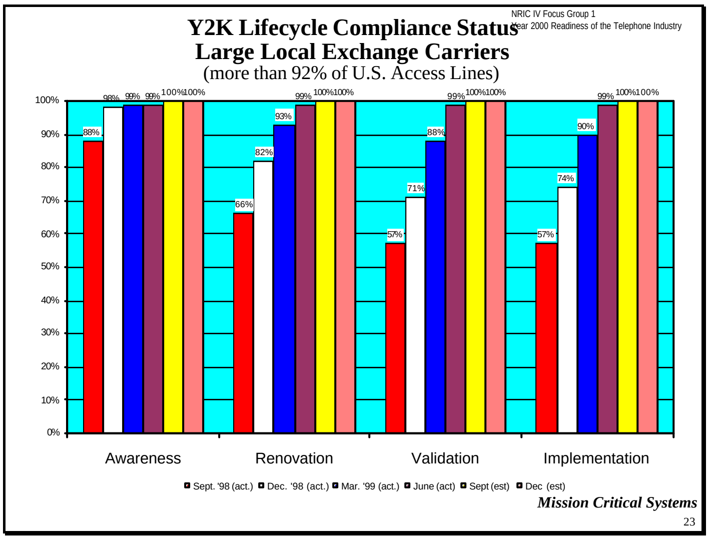


NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Backup Data

22

Slide 23



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

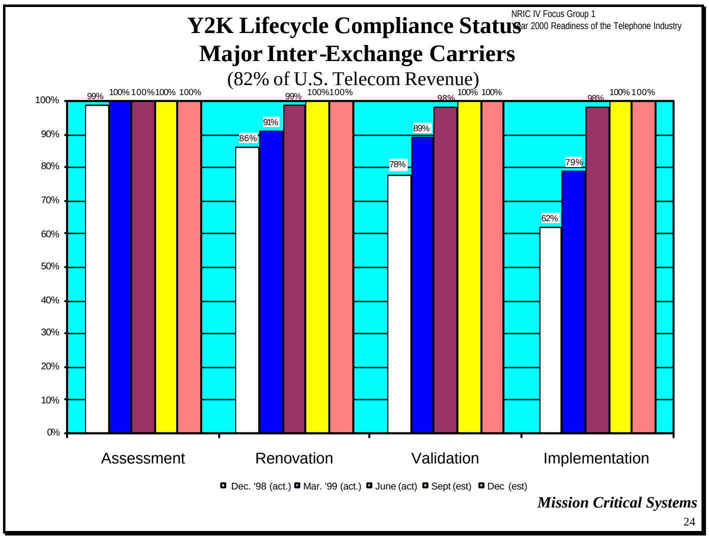
Y2K Lifecycle Compliance Status
Large Local Exchange Carriers

(more than 92% of U.S. Access Lines)

Mission Critical Systems

23

Slide 24



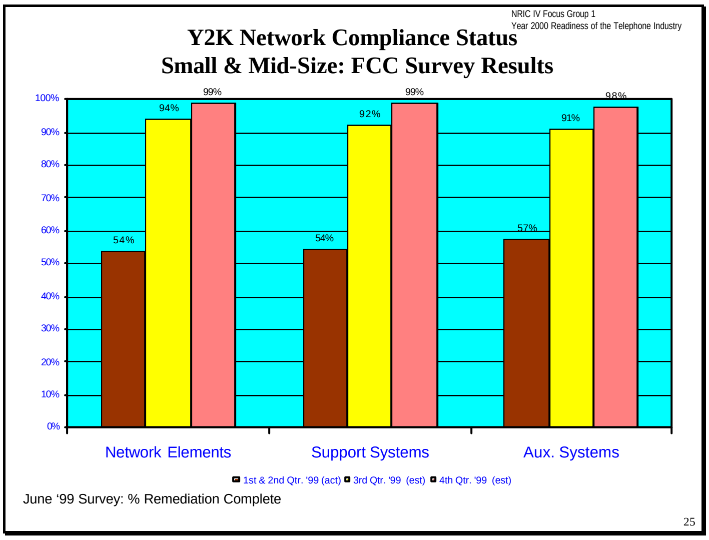
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Lifecycle Compliance Status
Major Inter-Exchange Carriers
(82% of U.S. Telecom Revenue)

Mission Critical Systems

24

Slide 25



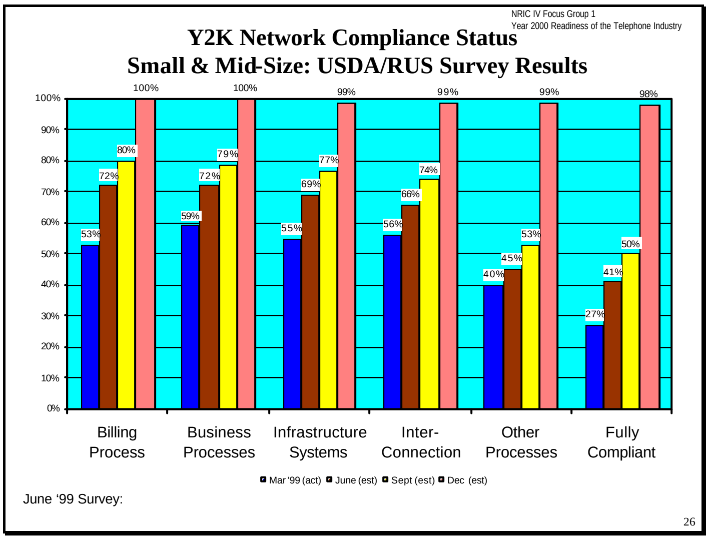
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Network Compliance Status
Small & Mid-Size: FCC Survey Results

June '99 Survey: % Remediation Complete

25

Slide 26



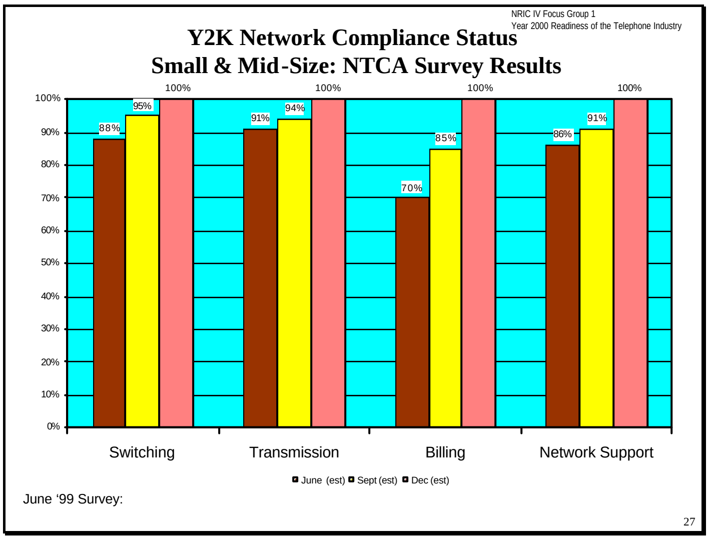
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Network Compliance Status
Small & Mid-Size: USDA/RUS Survey Results

June '99 Survey:

26

Slide 27



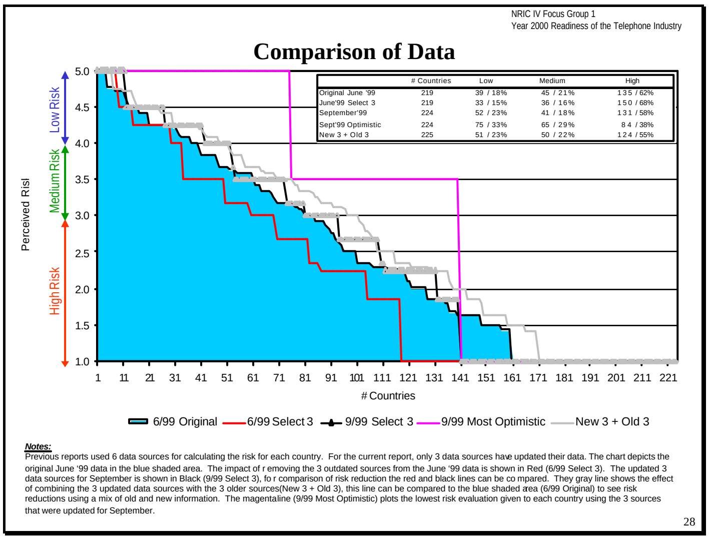
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Network Compliance Status
Small & Mid-Size: NTCA Survey Results

June '99 Survey:

27

Slide 28



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

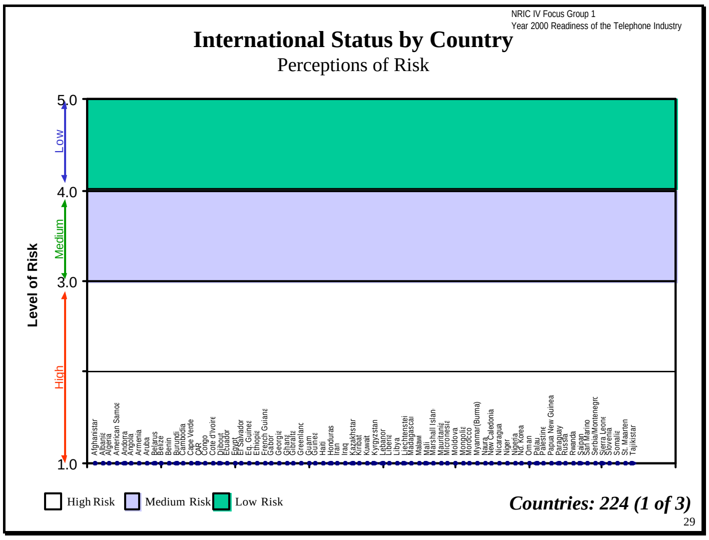
Comparison of Data

	# Countries	Low	Medium	High
Original June '99	219	39 / 18%	45 / 21%	135 / 62%
June'99 Select 3	219	33 / 15%	36 / 16%	150 / 68%
September'99	224	52 / 23%	41 / 18%	131 / 58%
Sept'99 Optimistic	224	75 / 33%	65 / 29%	84 / 38%
New 3 + Old 3	225	51 / 23%	50 / 22%	124 / 55%

Notes:
Previous reports used 6 data sources for calculating the risk for each country. For the current report, only 3 data sources have updated their data. The chart depicts the original June '99 data in the blue shaded area. The impact of removing the 3 outdated sources from the June '99 data is shown in Red (6/99 Select 3). The updated 3 data sources for September is shown in Black (9/99 Select 3), for comparison of risk reduction the red and black lines can be compared. They gray line shows the effect of combining the 3 updated data sources with the 3 older sources(New 3 + Old 3), this line can be compared to the blue shaded area (6/99 Original) to see risk reductions using a mix of old and new information. The magentaline (9/99 Most Optimistic) plots the lowest risk evaluation given to each country using the 3 sources that were updated for September.

28

Slide 29



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

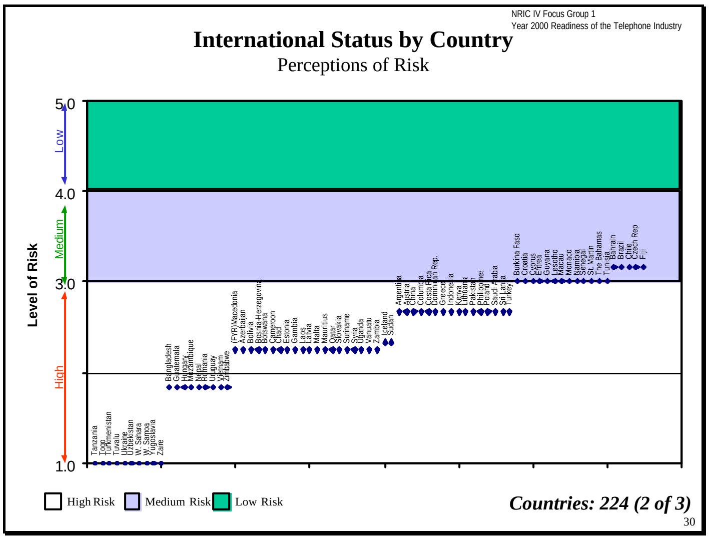
International Status by Country

Perceptions of Risk

Countries: 224 (1 of 3)

29

Slide 30



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

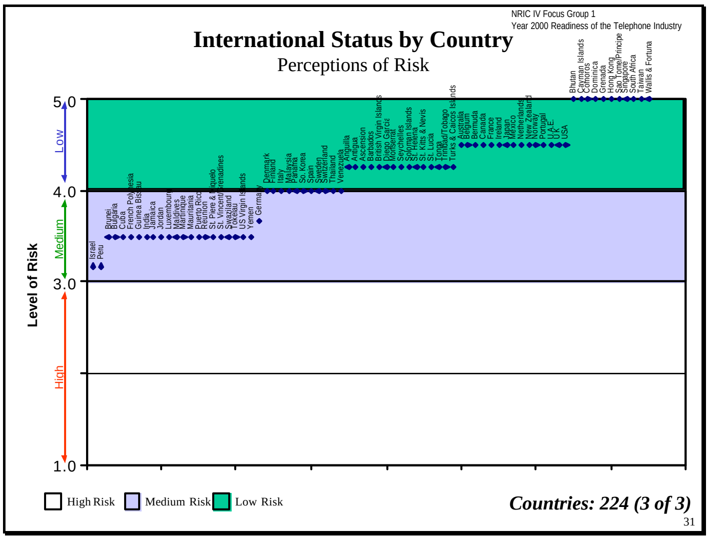
International Status by Country

Perceptions of Risk

Countries: 224 (2 of 3)

30

Slide 31



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

International Status by Country

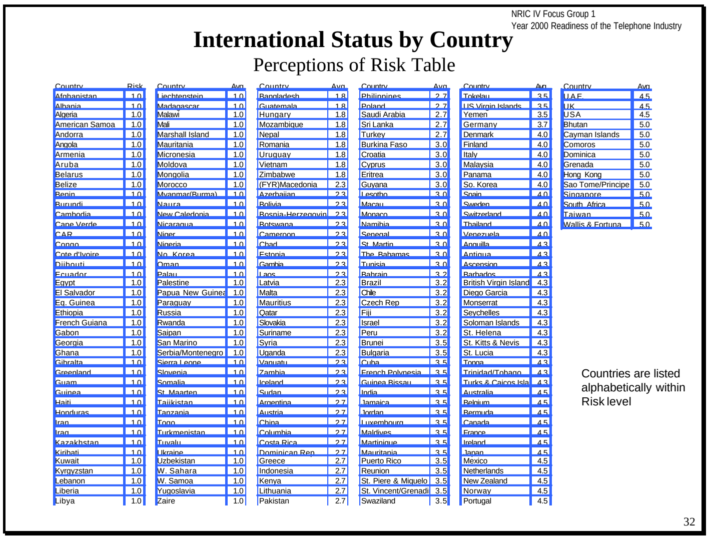
Perceptions of Risk

☐ High Risk ▨ Medium Risk 🟩 Low Risk

Countries: 224 (3 of 3)

31

Slide 32



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

International Status by Country

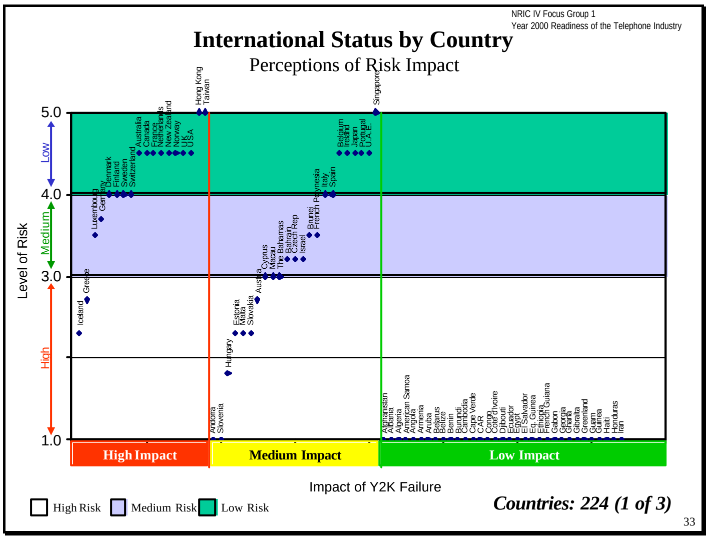
Perceptions of Risk Table

Country	Risk	Country	Avg	Country	Avg	Country	Avg	Country	Avg	Country	Avg
Afghanistan	1.0	Liechtenstein	1.0	Bangladesh	1.8	Philippines	2.7	Tokelau	3.5	U.A.E.	4.5
Albania	1.0	Madagascar	1.0	Guatemala	1.8	Poland	2.7	US Virgin Islands	3.5	UK	4.5
Algeria	1.0	Malawi	1.0	Hungary	1.8	Saudi Arabia	2.7	Yemen	3.5	USA	4.5
American Samoa	1.0	Mali	1.0	Mozambique	1.8	Sri Lanka	2.7	Germany	3.7	Bhutan	5.0
Andorra	1.0	Marshall Island	1.0	Nepal	1.8	Turkey	2.7	Denmark	4.0	Cayman Islands	5.0
Angola	1.0	Mauritania	1.0	Romania	1.8	Burkina Faso	3.0	Finland	4.0	Comoros	5.0
Armenia	1.0	Micronesia	1.0	Uruguay	1.8	Croatia	3.0	Italy	4.0	Dominica	5.0
Aruba	1.0	Moldova	1.0	Vietnam	1.8	Cyprus	3.0	Malaysia	4.0	Grenada	5.0
Belarus	1.0	Mongolia	1.0	Zimbabwe	1.8	Eritrea	3.0	Panama	4.0	Hong Kong	5.0
Belize	1.0	Morocco	1.0	(FYR)Macedonia	2.3	Guyana	3.0	So. Korea	4.0	Sao Tome/Principe	5.0
Benin	1.0	Myanmar(Burma)	1.0	Azerbaijan	2.3	Lesotho	3.0	Spain	4.0	Singapore	5.0
Burundi	1.0	Naura	1.0	Bolivia	2.3	Macau	3.0	Sweden	4.0	South Africa	5.0
Cambodia	1.0	New Caledonia	1.0	Bosnia-Herzegovin	2.3	Monaco	3.0	Switzerland	4.0	Taiwan	5.0
Cape Verde	1.0	Nicaragua	1.0	Botswana	2.3	Namibia	3.0	Thailand	4.0	Wallis & Fortuna	5.0
CAR	1.0	Niger	1.0	Cameroon	2.3	Senegal	3.0	Venezuela	4.0		
Congo	1.0	Nigeria	1.0	Chad	2.3	St. Martin	3.0	Anguilla	4.3		
Cote d'Ivoire	1.0	No. Korea	1.0	Estonia	2.3	The Bahamas	3.0	Antigua	4.3		
Djibouti	1.0	Oman	1.0	Gambia	2.3	Tunisia	3.0	Ascension	4.3		
Ecuador	1.0	Palau	1.0	Laos	2.3	Bahrain	3.2	Barbados	4.3		
Egypt	1.0	Palestine	1.0	Latvia	2.3	Brazil	3.2	British Virgin Island	4.3		
El Salvador	1.0	Papua New Guinea	1.0	Malta	2.3	Chile	3.2	Diego Garcia	4.3		
Eq. Guinea	1.0	Paraguay	1.0	Mauritius	2.3	Czech Rep	3.2	Monserrat	4.3		
Ethiopia	1.0	Russia	1.0	Qatar	2.3	Fiji	3.2	Seychelles	4.3		
French Guiana	1.0	Rwanda	1.0	Slovakia	2.3	Israel	3.2	Soloman Islands	4.3		
Gabon	1.0	Saipan	1.0	Suriname	2.3	Peru	3.2	St. Helena	4.3		
Georgia	1.0	San Marino	1.0	Syria	2.3	Brunei	3.5	St. Kitts & Nevis	4.3		
Ghana	1.0	Serbia/Montenegro	1.0	Uganda	2.3	Bulgaria	3.5	St. Lucia	4.3		
Gibralta	1.0	Sierra Leone	1.0	Vanuatu	2.3	Cuba	3.5	Tonga	4.3		
Greenland	1.0	Slovenia	1.0	Zambia	2.3	French Polynesia	3.5	Trinidad/Tobago	4.3		
Guam	1.0	Somalia	1.0	Iceland	2.3	Guinea Bissau	3.5	Turks & Caicos Isla	4.3		
Guinea	1.0	St. Maarten	1.0	Sudan	2.3	India	3.5	Australia	4.5		
Haiti	1.0	Tajikistan	1.0	Argentina	2.7	Jamaica	3.5	Belgium	4.5		
Honduras	1.0	Tanzania	1.0	Austria	2.7	Jordan	3.5	Bermuda	4.5		
Iran	1.0	Togo	1.0	China	2.7	Luxembourg	3.5	Canada	4.5		
Iraq	1.0	Turkmenistan	1.0	Columbia	2.7	Maldives	3.5	France	4.5		
Kazakhstan	1.0	Tuvalu	1.0	Costa Rica	2.7	Martinique	3.5	Ireland	4.5		
Kiribati	1.0	Ukraine	1.0	Dominican Rep	2.7	Mauritania	3.5	Japan	4.5		
Kuwait	1.0	Uzbekistan	1.0	Greece	2.7	Puerto Rico	3.5	Mexico	4.5		
Kyrgyzstan	1.0	W. Sahara	1.0	Indonesia	2.7	Reunion	3.5	Netherlands	4.5		
Lebanon	1.0	W. Samoa	1.0	Kenya	2.7	St. Piere & Miquelo	3.5	New Zealand	4.5		
Liberia	1.0	Yugoslavia	1.0	Lithuania	2.7	St. Vincent/Grenadi	3.5	Norway	4.5		
Libya	1.0	Zaire	1.0	Pakistan	2.7	Swaziland	3.5	Portugal	4.5		

Countries are listed alphabetically within Risk level

32

Slide 33



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

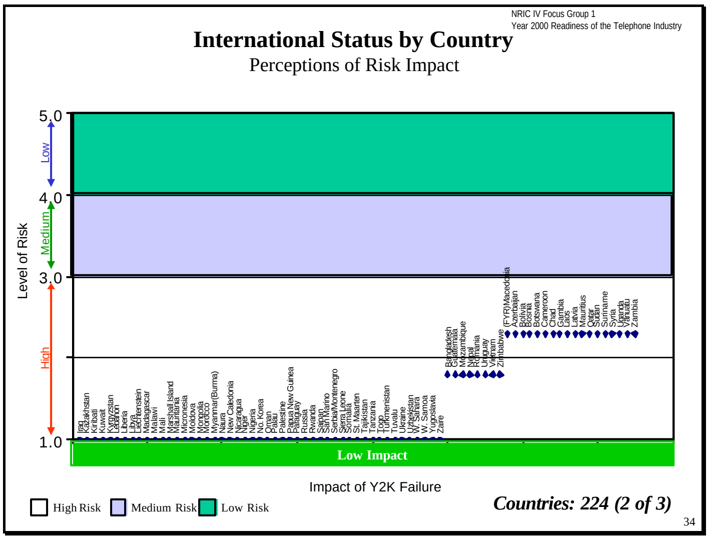
International Status by Country

Perceptions of Risk Impact

Countries: 224 (1 of 3)

33

Slide 34



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

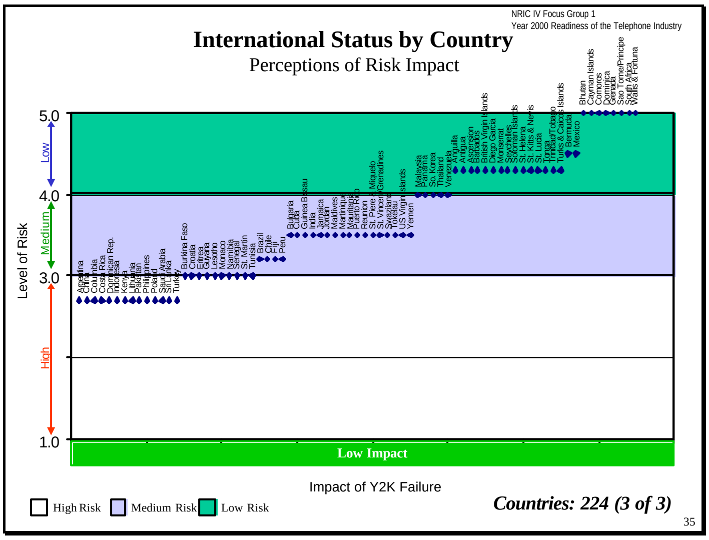
International Status by Country

Perceptions of Risk Impact

Countries: 224 (2 of 3)

34

Slide 35



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

International Status by Country

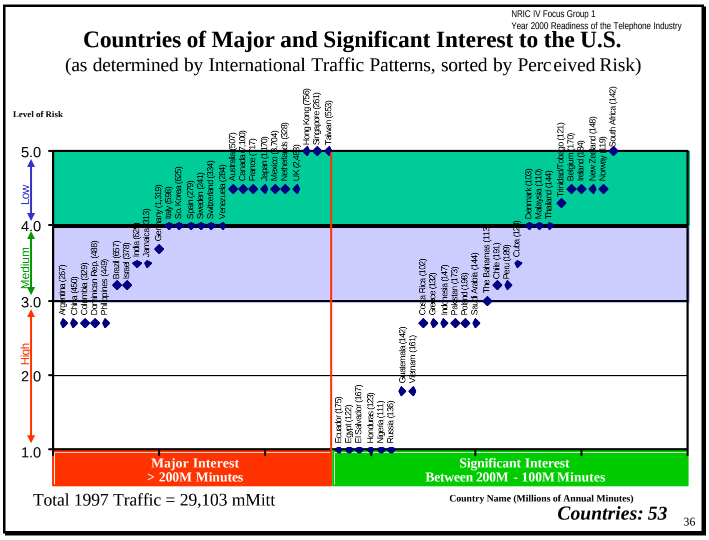
Perceptions of Risk Impact

□ High Risk ▨ Medium Risk 🟩 Low Risk

Countries: 224 (3 of 3)

35

Slide 36



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Countries of Major and Significant Interest to the U.S.

(as determined by International Traffic Patterns, sorted by Perceived Risk)

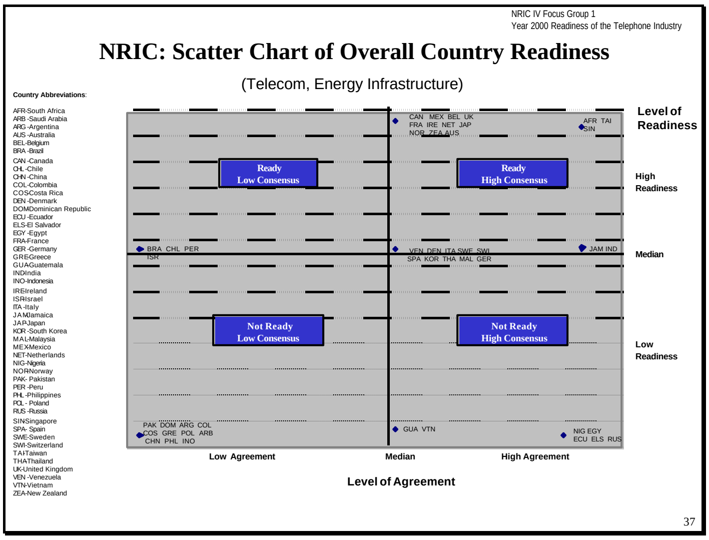
Total 1997 Traffic = 29,103 mMitt

Country Name (Millions of Annual Minutes)

Countries: 53

36

Slide 37



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

NRIC: Scatter Chart of Overall Country Readiness

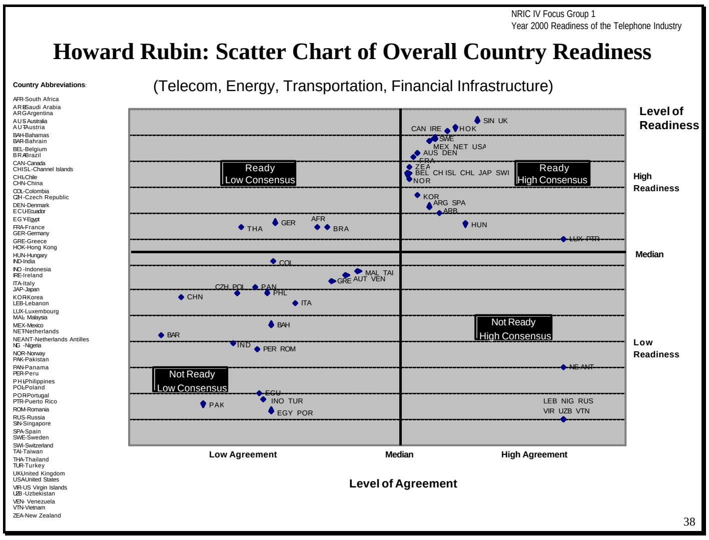
(Telecom, Energy Infrastructure)

Country Abbreviations:

AFR-South Africa
ARB -Saudi Arabia
ARG -Argentina
AUS -Australia
BEL-Belgium
BRA -Brazil
CAN -Canada
CHL -Chile
CHN -China
COL-Colombia
COSCosta Rica
DEN -Denmark
DOMDominican Republic
ECU -Ecuador
ELS-El Salvador
EGY -Egypt
FRA-France
GER -Germany
GREGreece
GUAGuatemala
INDIndia
INO-Indonesia
IREIreland
ISRIsrael
ITA -Italy
JAMJamaica
JAPJapan
KOR -South Korea
MALMalaysia
MEXMexico
NET-Netherlands
NIG-Nigeria
NORNorway
PAK- Pakistan
PER -Peru
PHL -Philippines
POL - Poland
RUS -Russia
SINSingapore
SPA- Spain
SWE-Sweden
SWI-Switzerland
TAITaiwan
THAThailand
UK-United Kingdom
VEN -Venezuela
VTN-Vietnam
ZEA-New Zealand

37

Slide 38



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Howard Rubin: Scatter Chart of Overall Country Readiness

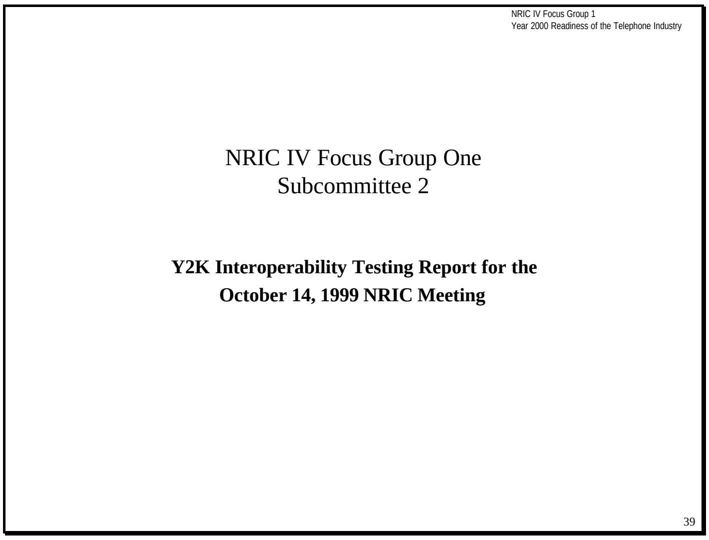
(Telecom, Energy, Transportation, Financial Infrastructure)

Country Abbreviations:

AFR-South Africa
ARB-Saudi Arabia
ARG-Argentina
AUS-Australia
AUT-Austria
BAH-Bahamas
BAR-Bahrain
BEL-Belgium
BRA-Brazil
CAN-Canada
CHISL-Channel Islands
CHL-Chile
CHN-China
COL-Colombia
CZH-Czech Republic
DEN-Denmark
ECU-Ecuador
EGY-Egypt
FRA-France
GER-Germany
GRE-Greece
HOK-Hong Kong
HUN-Hungary
IND-India
INO -Indonesia
IRE-Ireland
ITA-Italy
JAP-Japan
KOR-Korea
LEB-Lebanon
LUX-Luxembourg
MAL- Malaysia
MEX-Mexico
NET-Netherlands
NEANT-Netherlands Antilles
NG -Nigeria
NOR-Norway
PAK-Pakistan
PAN-Panama
PER-Peru
PHL-Philippines
POL-Poland
POR-Portugal
PTR-Puerto Rico
ROM-Romania
RUS-Russia
SIN-Singapore
SPA-Spain
SWE-Sweden
SWI-Switzerland
TAI-Taiwan
THA-Thailand
TUR-Turkey
UK-United Kingdom
USA-United States
VIR-US Virgin Islands
UZB -Uzbekistan
VEN- Venezuela
VTN-Vietnam
ZEA-New Zealand

38

Slide 39



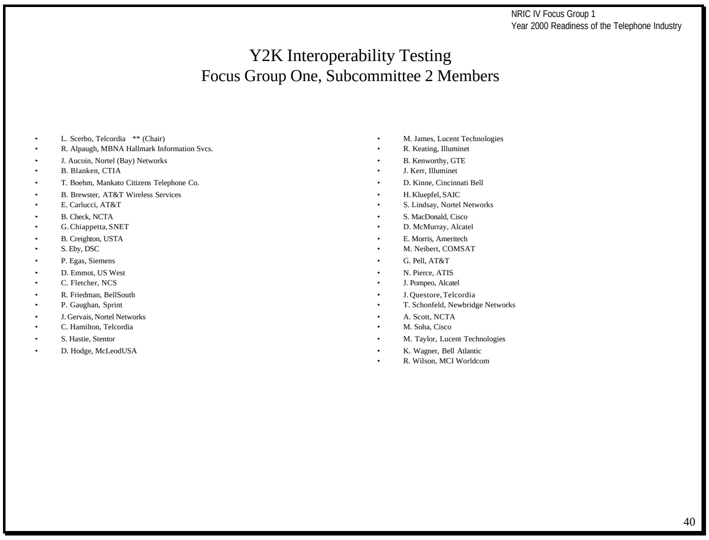
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

NRIC IV Focus Group One
Subcommittee 2

Y2K Interoperability Testing Report for the October 14, 1999 NRIC Meeting

39

Slide 40



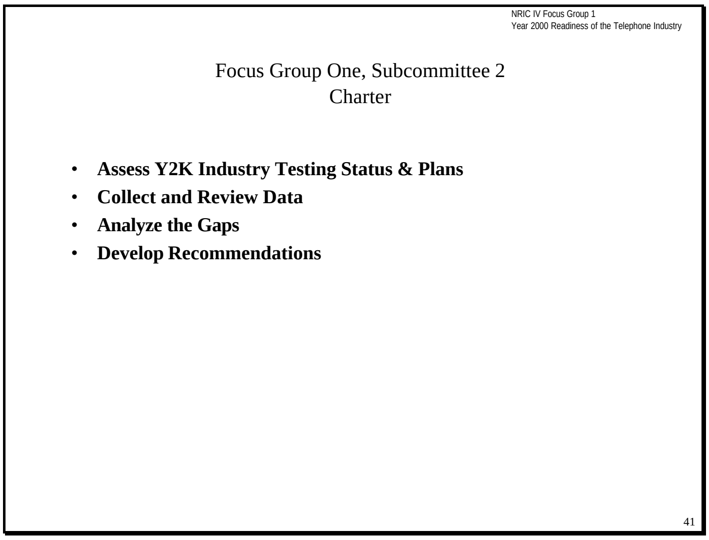
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Interoperability Testing
Focus Group One, Subcommittee 2 Members

- L. Scerbo, Telcordia ** (Chair)
- R. Alpaugh, MBNA Hallmark Information Svcs.
- J. Aucoin, Nortel (Bay) Networks
- B. Blanken, CTIA
- T. Boehm, Mankato Citizens Telephone Co.
- B. Brewster, AT&T Wireless Services
- E. Carlucci, AT&T
- B. Check, NCTA
- G. Chiappetta, SNET
- B. Creighton, USTA
- S. Eby, DSC
- P. Egas, Siemens
- D. Emmot, US West
- C. Fletcher, NCS
- R. Friedman, BellSouth
- P. Gaughan, Sprint
- J. Gervais, Nortel Networks
- C. Hamilton, Telcordia
- S. Hastie, Stentor
- D. Hodge, McLeodUSA
- M. James, Lucent Technologies
- R. Keating, Illuminet
- B. Kenworthy, GTE
- J. Kerr, Illuminet
- D. Kinne, Cincinnati Bell
- H. Kluepfel, SAIC
- S. Lindsay, Nortel Networks
- S. MacDonald, Cisco
- D. McMurray, Alcatel
- E. Morris, Ameritech
- M. Neibert, COMSAT
- G. Pell, AT&T
- N. Pierce, ATIS
- J. Pompeo, Alcatel
- J. Questore, Telcordia
- T. Schonfeld, Newbridge Networks
- A. Scott, NCTA
- M. Soha, Cisco
- M. Taylor, Lucent Technologies
- K. Wagner, Bell Atlantic
- R. Wilson, MCI Worldcom

40

Slide 41



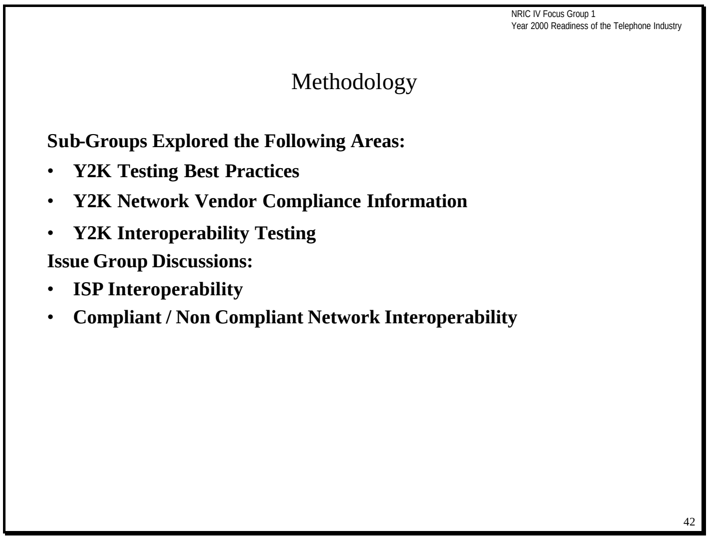
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Focus Group One, Subcommittee 2
Charter

- **Assess Y2K Industry Testing Status & Plans**
- **Collect and Review Data**
- **Analyze the Gaps**
- **Develop Recommendations**

41

Slide 42



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Methodology

Sub-Groups Explored the Following Areas:

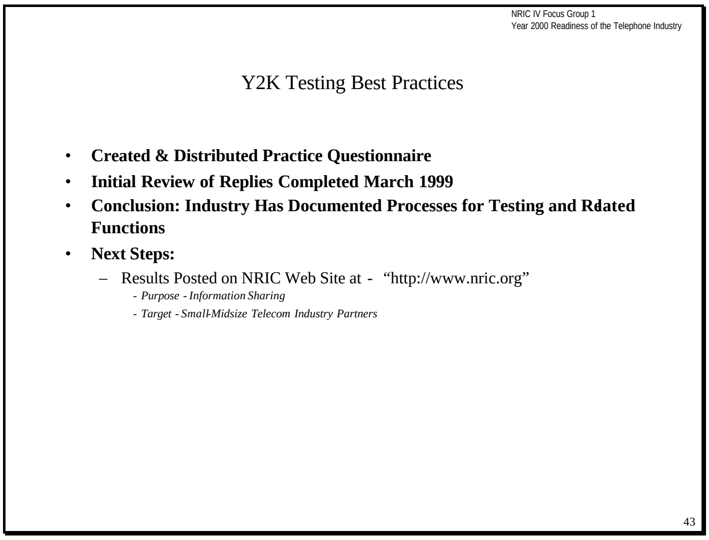
- **Y2K Testing Best Practices**
- **Y2K Network Vendor Compliance Information**
- **Y2K Interoperability Testing**

Issue Group Discussions:

- **ISP Interoperability**
- **Compliant / Non Compliant Network Interoperability**

42

Slide 43



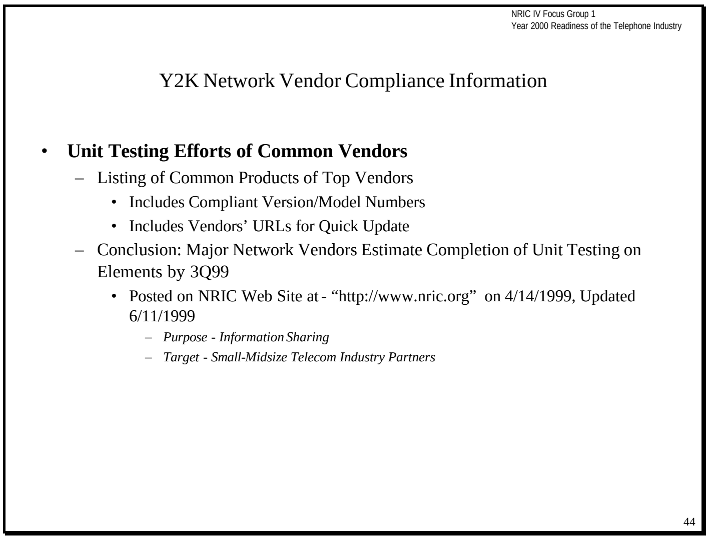
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Testing Best Practices

- **Created & Distributed Practice Questionnaire**
- **Initial Review of Replies Completed March 1999**
- **Conclusion: Industry Has Documented Processes for Testing and Related Functions**
- **Next Steps:**
  - Results Posted on NRIC Web Site at - "http://www.nric.org"
    - *Purpose - Information Sharing*
    - *Target - Small-Midsize Telecom Industry Partners*

43

Slide 44



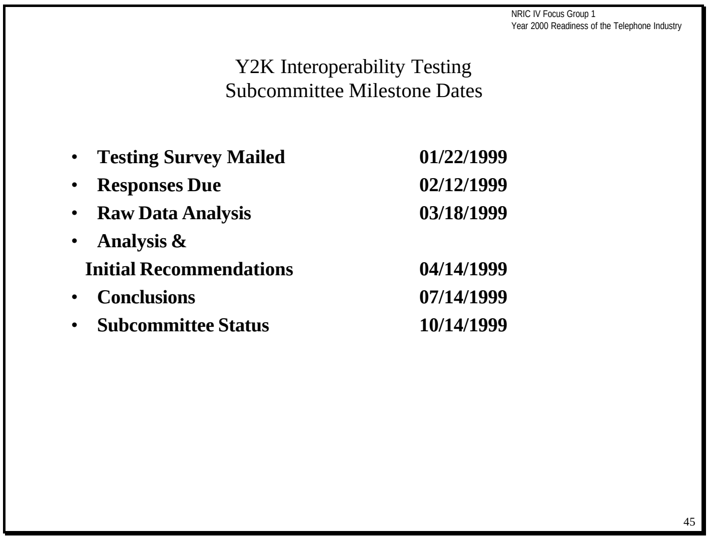
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Network Vendor Compliance Information

- **Unit Testing Efforts of Common Vendors**
  - Listing of Common Products of Top Vendors
    - Includes Compliant Version/Model Numbers
    - Includes Vendors' URLs for Quick Update
  - Conclusion: Major Network Vendors Estimate Completion of Unit Testing on Elements by 3Q99
    - Posted on NRIC Web Site at - "http://www.nric.org" on 4/14/1999, Updated 6/11/1999
      - *Purpose - Information Sharing*
      - *Target - Small-Midsize Telecom Industry Partners*

44

Slide 45



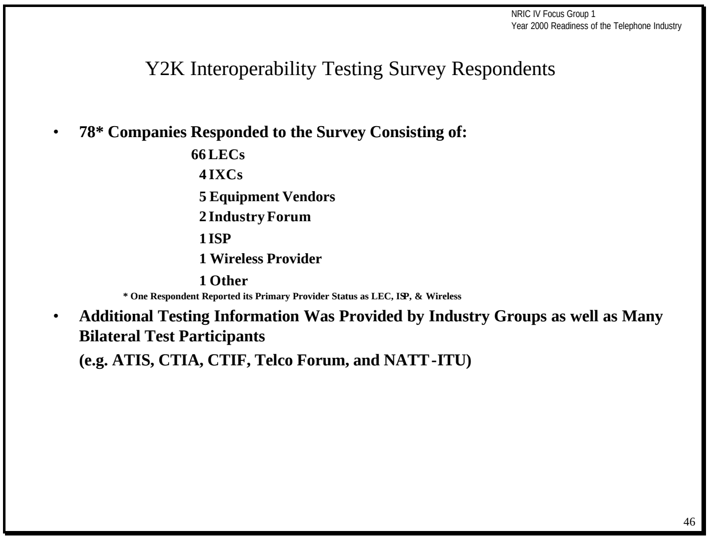
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Interoperability Testing
Subcommittee Milestone Dates

• **Testing Survey Mailed**	**01/22/1999**
• **Responses Due**	**02/12/1999**
• **Raw Data Analysis**	**03/18/1999**
• **Analysis &** **Initial Recommendations**	**04/14/1999**
• **Conclusions**	**07/14/1999**
• **Subcommittee Status**	**10/14/1999**

45

Slide 46



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Interoperability Testing Survey Respondents

- **78* Companies Responded to the Survey Consisting of:**

  66 LECs
  4 IXCs
  5 Equipment Vendors
  2 Industry Forum
  1 ISP
  1 Wireless Provider
  1 Other

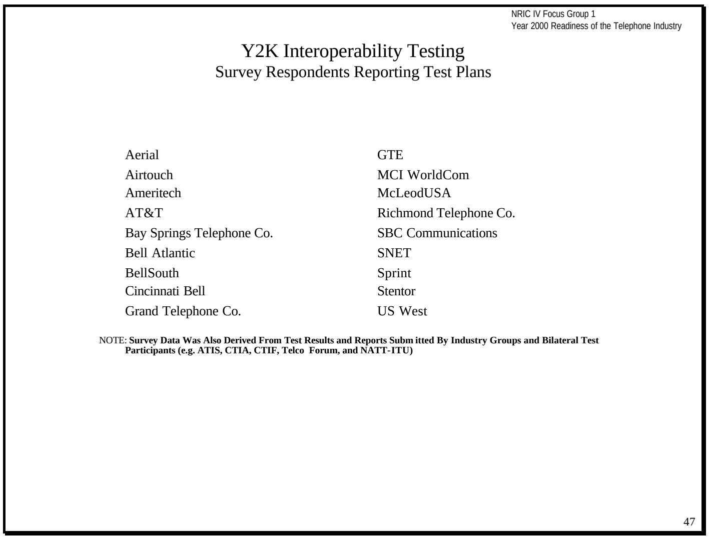
  *** One Respondent Reported its Primary Provider Status as LEC, ISP, & Wireless**

- **Additional Testing Information Was Provided by Industry Groups as well as Many Bilateral Test Participants**

  (e.g. ATIS, CTIA, CTIF, Telco Forum, and NATT-ITU)

46

Slide 47



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

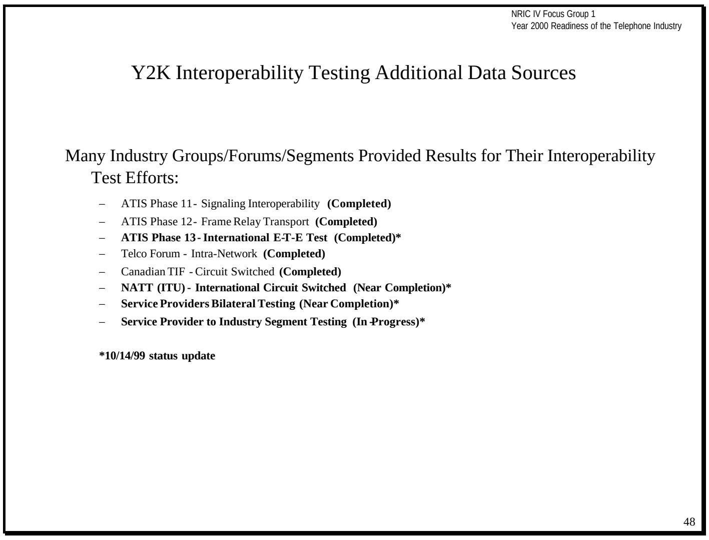
Y2K Interoperability Testing
Survey Respondents Reporting Test Plans

- Aerial
- Airtouch
- Ameritech
- AT&T
- Bay Springs Telephone Co.
- Bell Atlantic
- BellSouth
- Cincinnati Bell
- Grand Telephone Co.
- GTE
- MCI WorldCom
- McLeodUSA
- Richmond Telephone Co.
- SBC Communications
- SNET
- Sprint
- Stentor
- US West

NOTE: **Survey Data Was Also Derived From Test Results and Reports Subm itted By Industry Groups and Bilateral Test Participants (e.g. ATIS, CTIA, CTIF, Telco Forum, and NATT-ITU)**

47

Slide 48



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Interoperability Testing Additional Data Sources

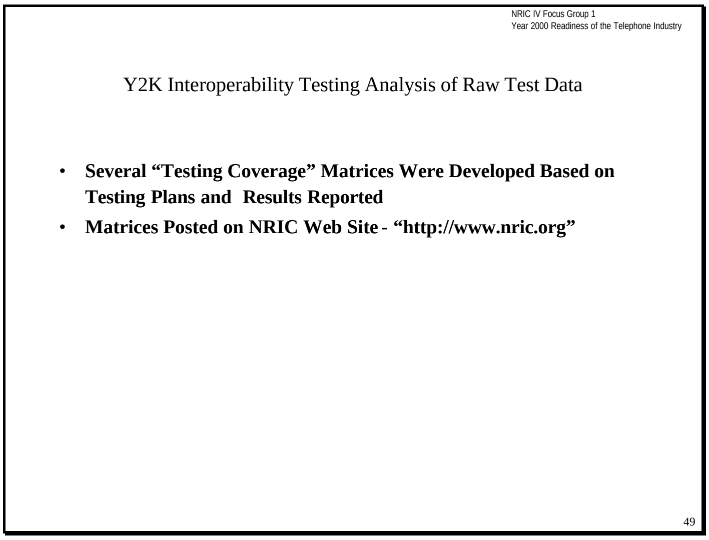
Many Industry Groups/Forums/Segments Provided Results for Their Interoperability Test Efforts:

- ATIS Phase 11 - Signaling Interoperability **(Completed)**
- ATIS Phase 12 - Frame Relay Transport **(Completed)**
- **ATIS Phase 13 - International E-T-E Test (Completed)***
- Telco Forum - Intra-Network **(Completed)**
- Canadian TIF - Circuit Switched **(Completed)**
- **NATT (ITU) - International Circuit Switched (Near Completion)***
- **Service Providers Bilateral Testing (Near Completion)***
- **Service Provider to Industry Segment Testing (In -Progress)***

***10/14/99 status update**

48

Slide 49



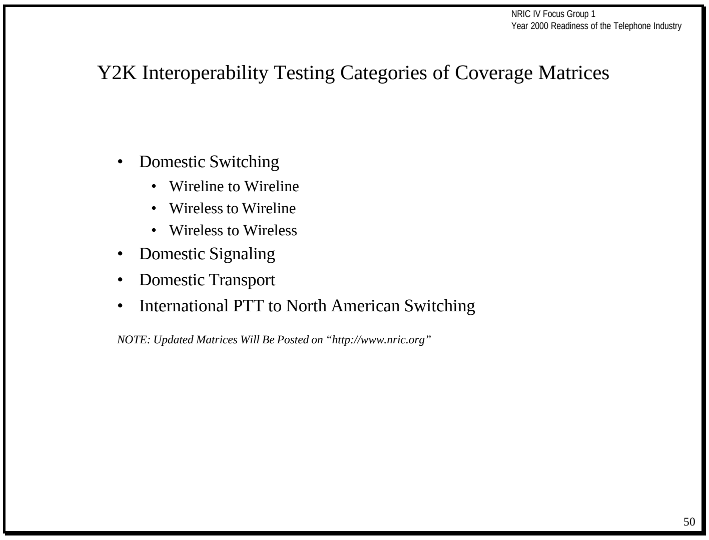
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Interoperability Testing Analysis of Raw Test Data

- **Several "Testing Coverage" Matrices Were Developed Based on Testing Plans and Results Reported**
- **Matrices Posted on NRIC Web Site - "http://www.nric.org"**

49

Slide 50



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

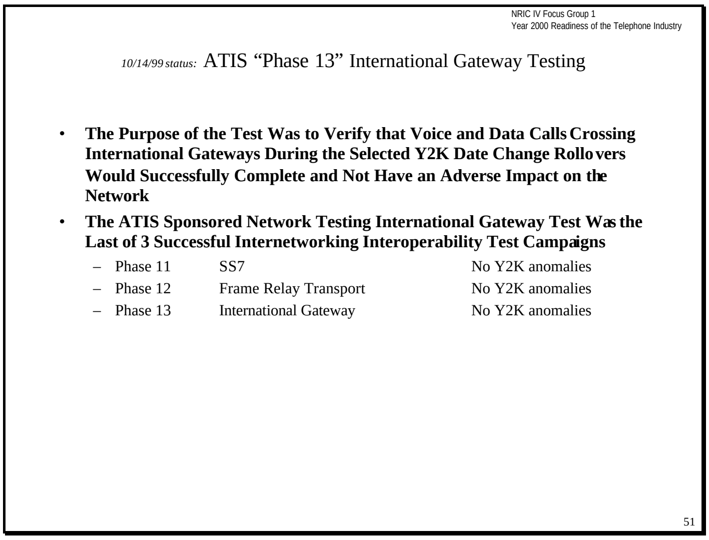
Y2K Interoperability Testing Categories of Coverage Matrices

- Domestic Switching
  - Wireline to Wireline
  - Wireless to Wireline
  - Wireless to Wireless
- Domestic Signaling
- Domestic Transport
- International PTT to North American Switching

NOTE: Updated Matrices Will Be Posted on “http://www.nric.org”

50

Slide 51

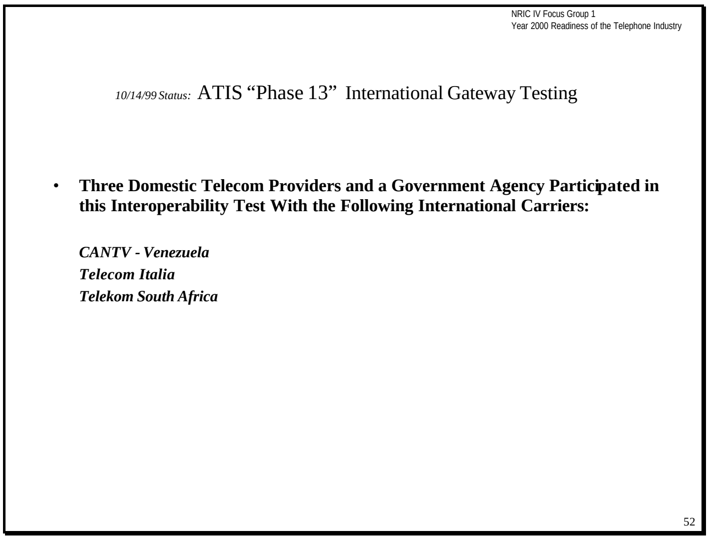


10/14/99 status: ATIS “Phase 13” International Gateway Testing

- **The Purpose of the Test Was to Verify that Voice and Data Calls Crossing International Gateways During the Selected Y2K Date Change Rollovers Would Successfully Complete and Not Have an Adverse Impact on the Network**
- **The ATIS Sponsored Network Testing International Gateway Test Was the Last of 3 Successful Internetworking Interoperability Test Campaigns**

– Phase 11	SS7	No Y2K anomalies
– Phase 12	Frame Relay Transport	No Y2K anomalies
– Phase 13	International Gateway	No Y2K anomalies

Slide 52



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

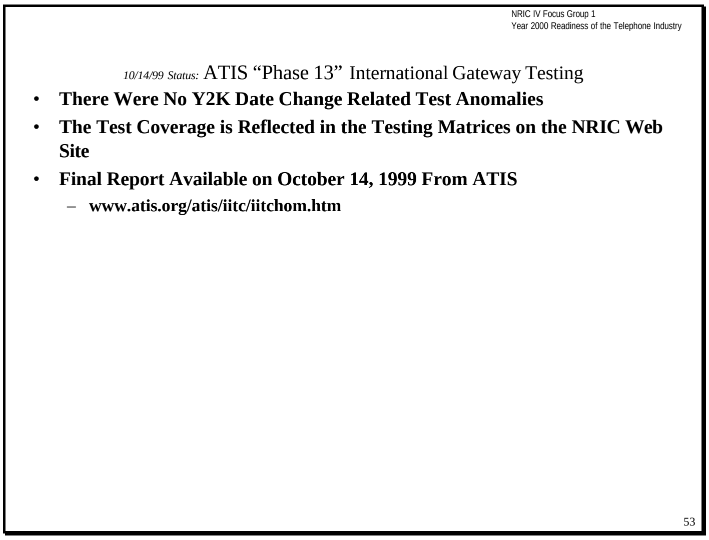
10/14/99 Status: ATIS “Phase 13” International Gateway Testing

- **Three Domestic Telecom Providers and a Government Agency Participated in this Interoperability Test With the Following International Carriers:**

CANTV - Venezuela
Telecom Italia
Telekom South Africa

52

Slide 53



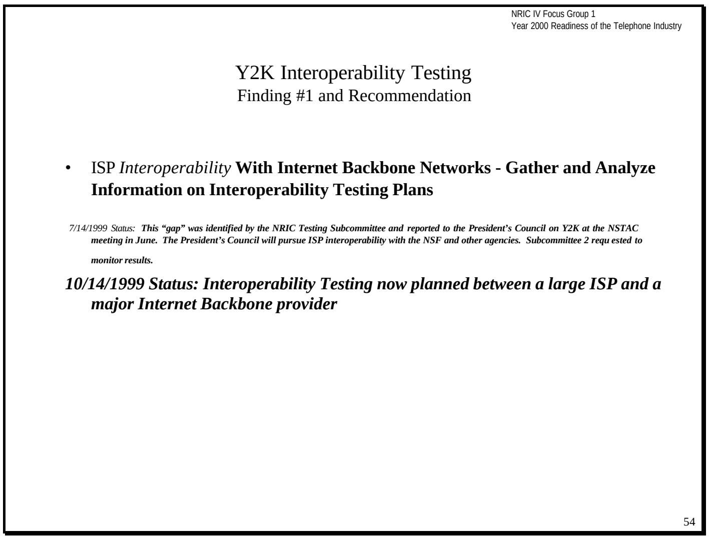
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

10/14/99 Status: ATIS “Phase 13” International Gateway Testing

- **There Were No Y2K Date Change Related Test Anomalies**
- **The Test Coverage is Reflected in the Testing Matrices on the NRIC Web Site**
- **Final Report Available on October 14, 1999 From ATIS**
  - **www.atis.org/atis/iitc/iitchom.htm**

53

Slide 54



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Interoperability Testing
Finding #1 and Recommendation

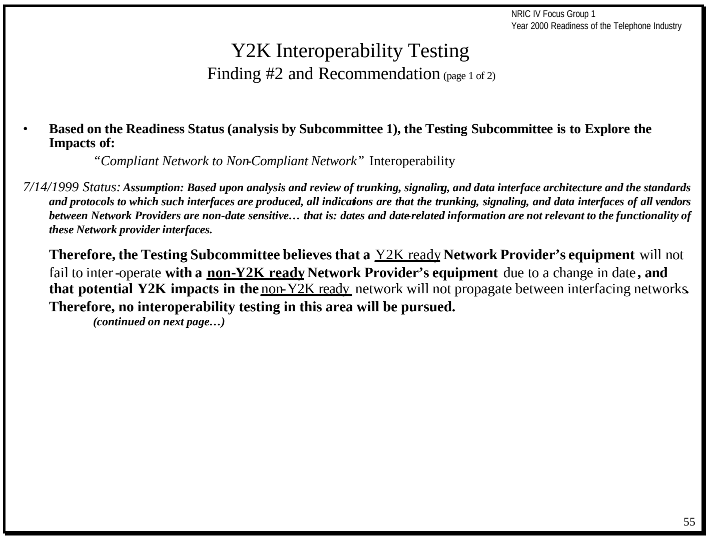
- ISP *Interoperability* **With Internet Backbone Networks - Gather and Analyze Information on Interoperability Testing Plans**

7/14/1999 Status: ***This "gap" was identified by the NRIC Testing Subcommittee and reported to the President's Council on Y2K at the NSTAC meeting in June. The President's Council will pursue ISP interoperability with the NSF and other agencies. Subcommittee 2 requ ested to monitor results.***

10/14/1999 Status: Interoperability Testing now planned between a large ISP and a major Internet Backbone provider

54

Slide 55



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Interoperability Testing

Finding #2 and Recommendation (page 1 of 2)

- **Based on the Readiness Status (analysis by Subcommittee 1), the Testing Subcommittee is to Explore the Impacts of:**

  "Compliant Network to Non-Compliant Network" Interoperability

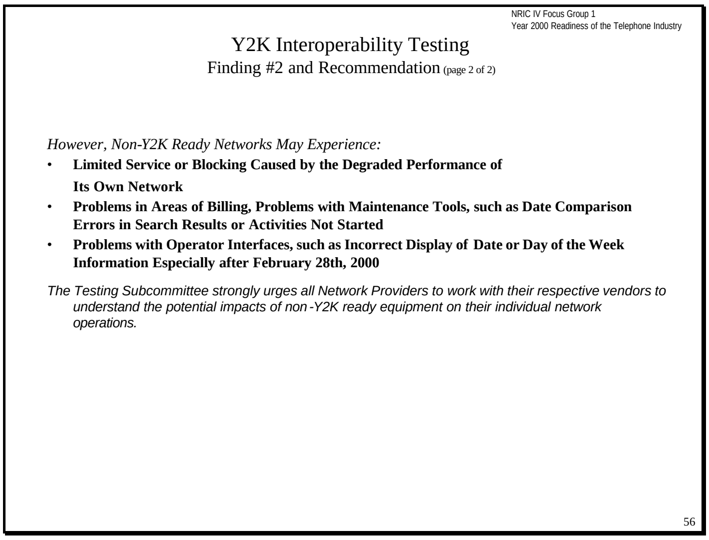
7/14/1999 Status: ***Assumption: Based upon analysis and review of trunking, signaling, and data interface architecture and the standards and protocols to which such interfaces are produced, all indications are that the trunking, signaling, and data interfaces of all vendors between Network Providers are non-date sensitive… that is: dates and date-related information are not relevant to the functionality of these Network provider interfaces.***

Therefore, the Testing Subcommittee believes that a Y2K ready **Network Provider's equipment** will not fail to inter-operate **with a non-Y2K ready Network Provider's equipment** due to a change in date**, and that potential Y2K impacts in the** non-Y2K ready network will not propagate between interfacing networks. **Therefore, no interoperability testing in this area will be pursued.**

(continued on next page…)

55

Slide 56



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Interoperability Testing

Finding #2 and Recommendation (page 2 of 2)

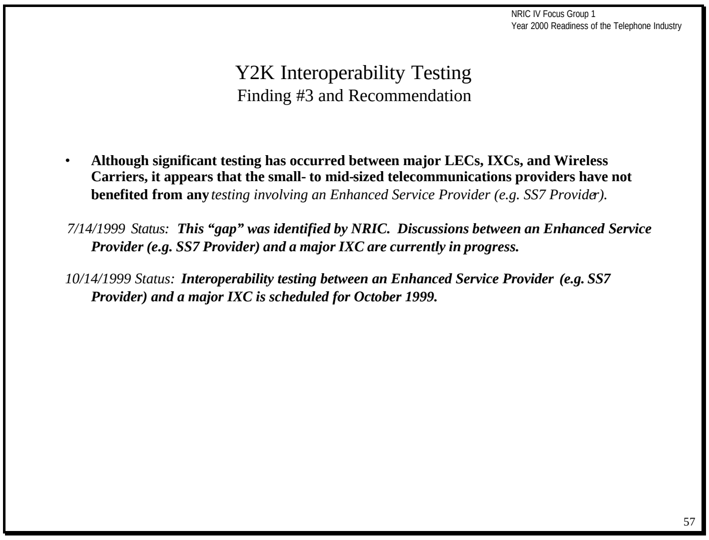
However, Non-Y2K Ready Networks May Experience:

- **Limited Service or Blocking Caused by the Degraded Performance of Its Own Network**
- **Problems in Areas of Billing, Problems with Maintenance Tools, such as Date Comparison Errors in Search Results or Activities Not Started**
- **Problems with Operator Interfaces, such as Incorrect Display of Date or Day of the Week Information Especially after February 28th, 2000**

The Testing Subcommittee strongly urges all Network Providers to work with their respective vendors to understand the potential impacts of non -Y2K ready equipment on their individual network operations.

56

Slide 57



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Y2K Interoperability Testing

Finding #3 and Recommendation

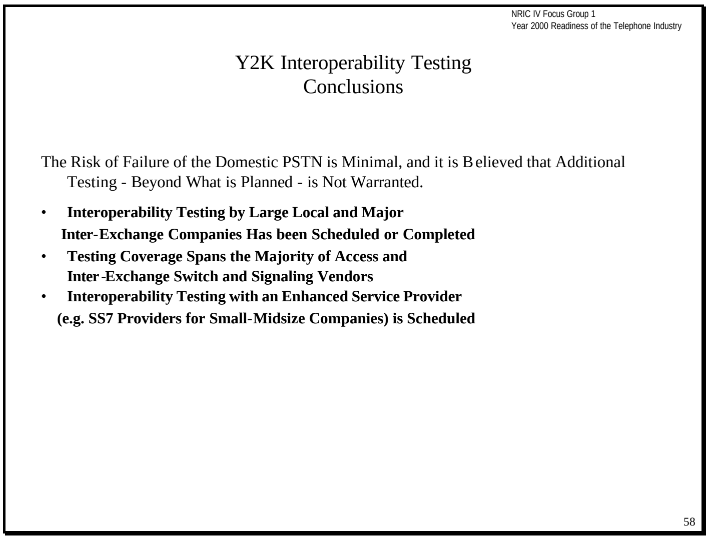
- **Although significant testing has occurred between major LECs, IXCs, and Wireless Carriers, it appears that the small- to mid-sized telecommunications providers have not benefited from any** *testing involving an Enhanced Service Provider (e.g. SS7 Provider).*

7/14/1999 Status: ***This "gap" was identified by NRIC. Discussions between an Enhanced Service Provider (e.g. SS7 Provider) and a major IXC are currently in progress.***

10/14/1999 Status: ***Interoperability testing between an Enhanced Service Provider (e.g. SS7 Provider) and a major IXC is scheduled for October 1999.***

57

Slide 58



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

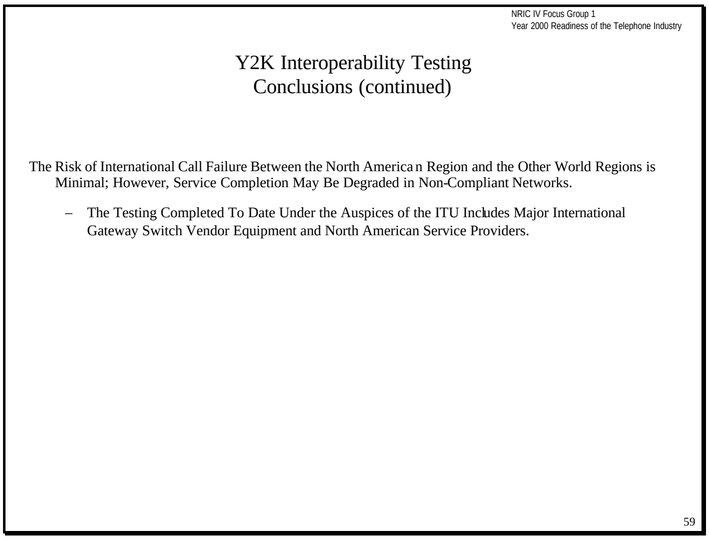
Y2K Interoperability Testing Conclusions

The Risk of Failure of the Domestic PSTN is Minimal, and it is Believed that Additional Testing - Beyond What is Planned - is Not Warranted.

- **Interoperability Testing by Large Local and Major Inter-Exchange Companies Has been Scheduled or Completed**
- **Testing Coverage Spans the Majority of Access and Inter-Exchange Switch and Signaling Vendors**
- **Interoperability Testing with an Enhanced Service Provider (e.g. SS7 Providers for Small-Midsize Companies) is Scheduled**

58

Slide 59



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

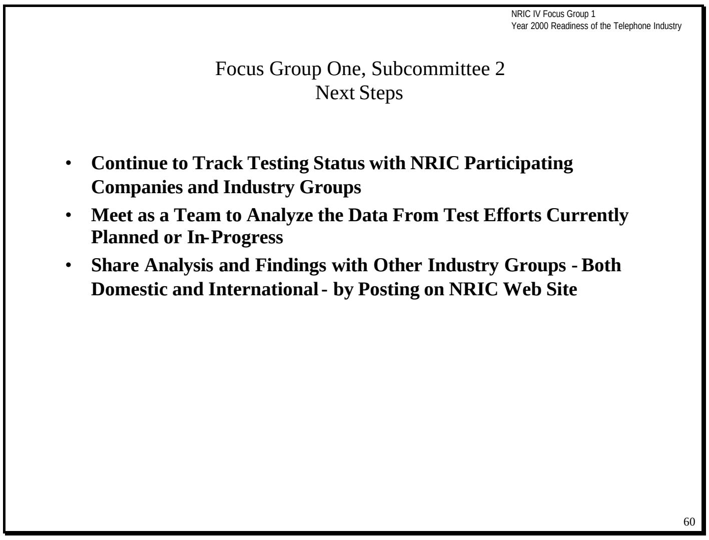
Y2K Interoperability Testing Conclusions (continued)

The Risk of International Call Failure Between the North America n Region and the Other World Regions is Minimal; However, Service Completion May Be Degraded in Non-Compliant Networks.

- The Testing Completed To Date Under the Auspices of the ITU Includes Major International Gateway Switch Vendor Equipment and North American Service Providers.

59

Slide 60



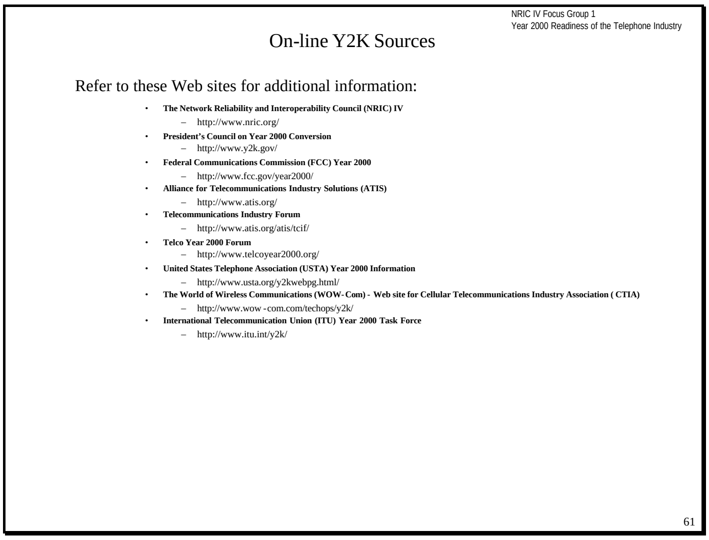
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Focus Group One, Subcommittee 2
Next Steps

- **Continue to Track Testing Status with NRIC Participating Companies and Industry Groups**
- **Meet as a Team to Analyze the Data From Test Efforts Currently Planned or In-Progress**
- **Share Analysis and Findings with Other Industry Groups - Both Domestic and International - by Posting on NRIC Web Site**

60

Slide 61



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

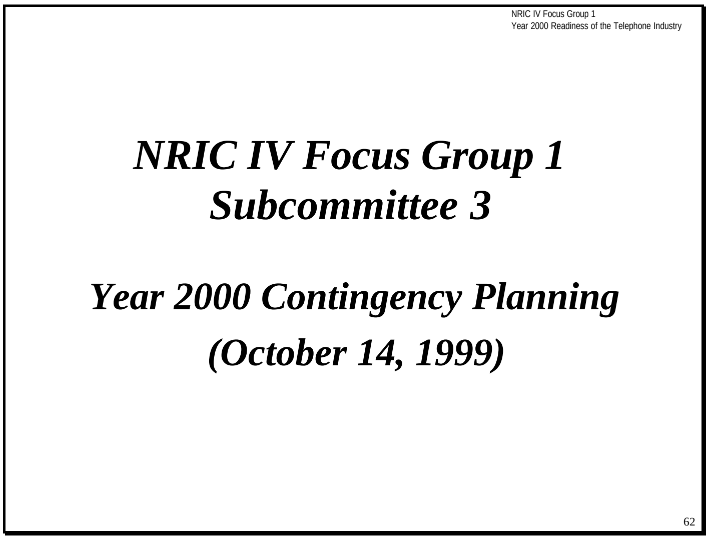
On-line Y2K Sources

Refer to these Web sites for additional information:

- **The Network Reliability and Interoperability Council (NRIC) IV**
  - http://www.nric.org/
- **President's Council on Year 2000 Conversion**
  - http://www.y2k.gov/
- **Federal Communications Commission (FCC) Year 2000**
  - http://www.fcc.gov/year2000/
- **Alliance for Telecommunications Industry Solutions (ATIS)**
  - http://www.atis.org/
- **Telecommunications Industry Forum**
  - http://www.atis.org/atis/tcif/
- **Telco Year 2000 Forum**
  - http://www.telcoyear2000.org/
- **United States Telephone Association (USTA) Year 2000 Information**
  - http://www.usta.org/y2kwebpg.html/
- **The World of Wireless Communications (WOW-Com) - Web site for Cellular Telecommunications Industry Association (CTIA)**
  - http://www.wow -com.com/techops/y2k/
- **International Telecommunication Union (ITU) Year 2000 Task Force**
  - http://www.itu.int/y2k/

61

Slide 62



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

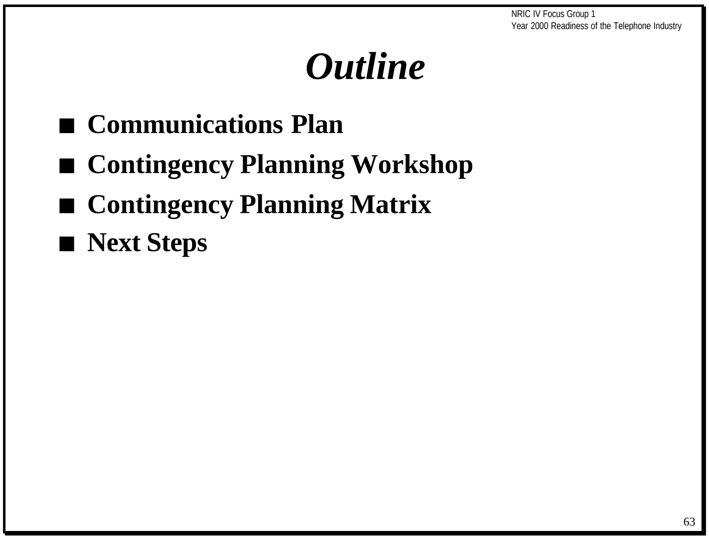
NRIC IV Focus Group 1
Subcommittee 3

Year 2000 Contingency Planning

(October 14, 1999)

62

Slide 63

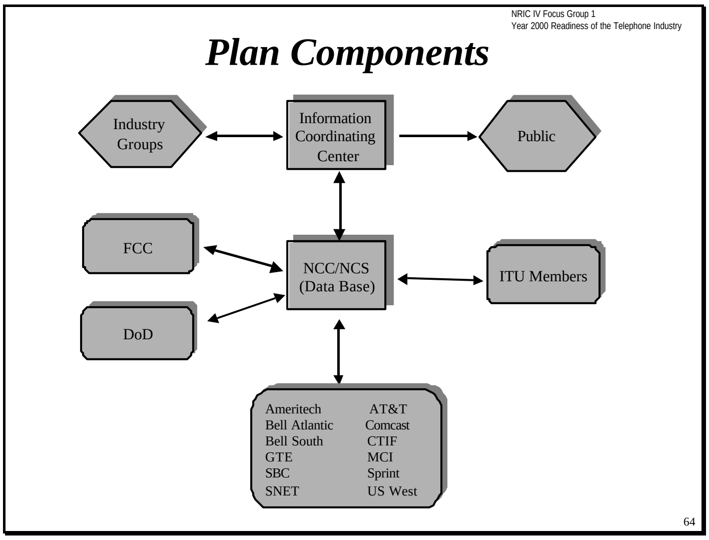


NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Outline

- Communications Plan
- Contingency Planning Workshop
- Contingency Planning Matrix
- Next Steps

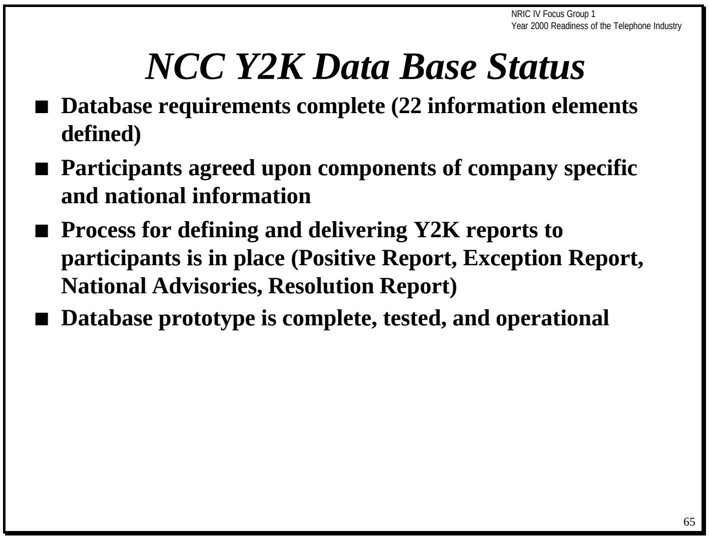
Slide 64



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Plan Components

Slide 65



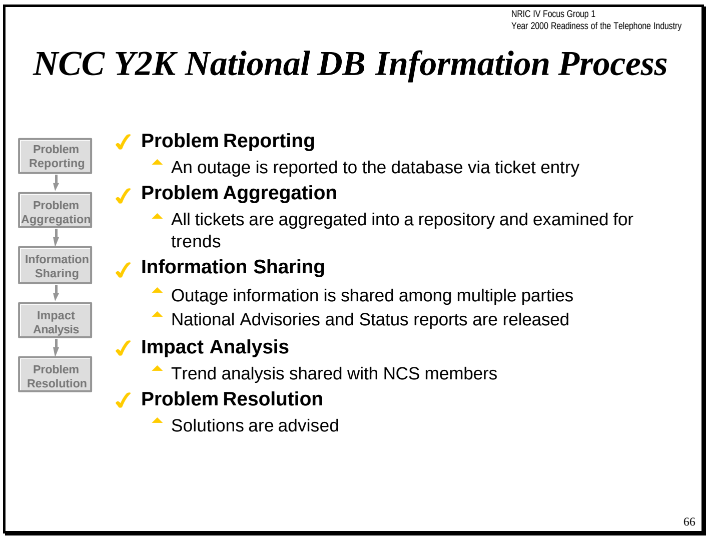
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

NCC Y2K Data Base Status

- **Database requirements complete (22 information elements defined)**
- **Participants agreed upon components of company specific and national information**
- **Process for defining and delivering Y2K reports to participants is in place (Positive Report, Exception Report, National Advisories, Resolution Report)**
- **Database prototype is complete, tested, and operational**

65

Slide 66



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

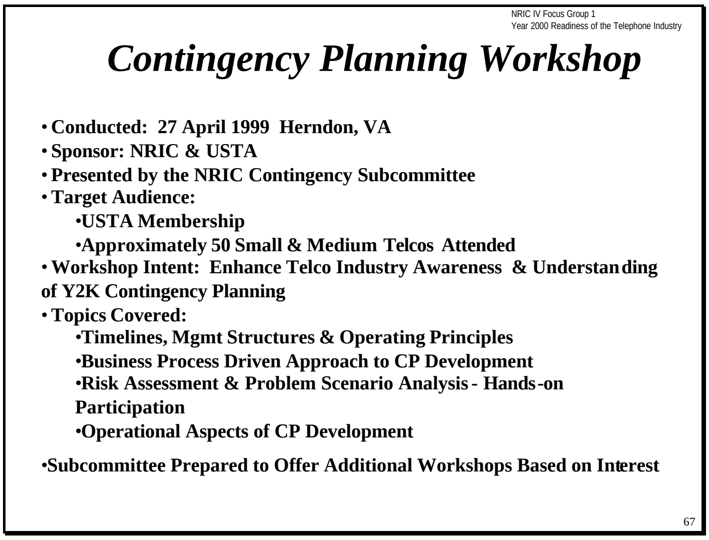
NCC Y2K National DB Information Process

Problem Reporting → Problem Aggregation → Information Sharing → Impact Analysis → Problem Resolution

- ✓ **Problem Reporting**
  - An outage is reported to the database via ticket entry
- ✓ **Problem Aggregation**
  - All tickets are aggregated into a repository and examined for trends
- ✓ **Information Sharing**
  - Outage information is shared among multiple parties
  - National Advisories and Status reports are released
- ✓ **Impact Analysis**
  - Trend analysis shared with NCS members
- ✓ **Problem Resolution**
  - Solutions are advised

66

Slide 67



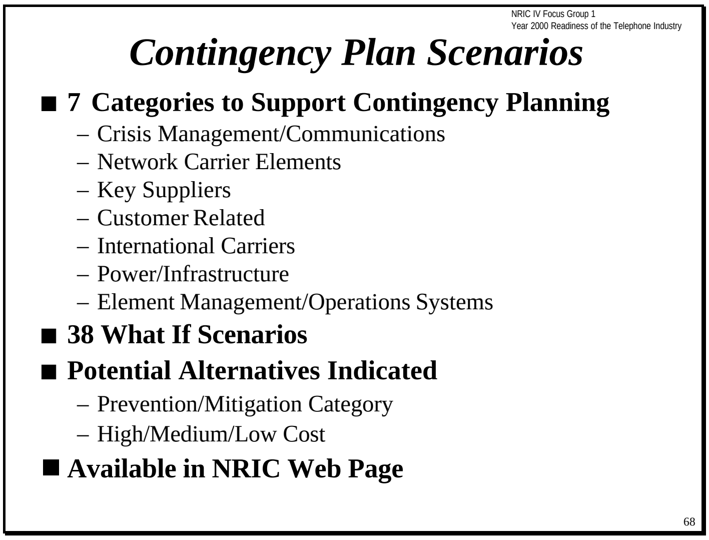
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Contingency Planning Workshop

- **Conducted: 27 April 1999 Herndon, VA**
- **Sponsor: NRIC & USTA**
- **Presented by the NRIC Contingency Subcommittee**
- **Target Audience:**
  - **USTA Membership**
  - **Approximately 50 Small & Medium Telcos Attended**
- **Workshop Intent: Enhance Telco Industry Awareness & Understanding of Y2K Contingency Planning**
- **Topics Covered:**
  - **Timelines, Mgmt Structures & Operating Principles**
  - **Business Process Driven Approach to CP Development**
  - **Risk Assessment & Problem Scenario Analysis - Hands-on Participation**
  - **Operational Aspects of CP Development**
- **Subcommittee Prepared to Offer Additional Workshops Based on Interest**

67

Slide 68



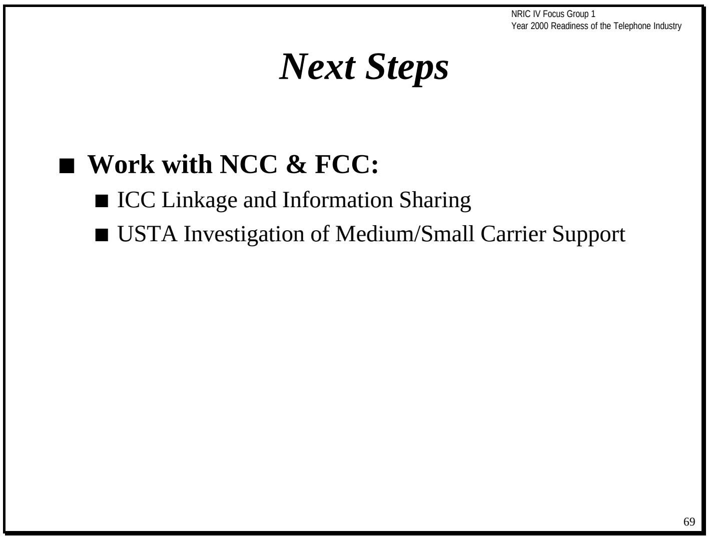
NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Contingency Plan Scenarios

- **7 Categories to Support Contingency Planning**
  - Crisis Management/Communications
  - Network Carrier Elements
  - Key Suppliers
  - Customer Related
  - International Carriers
  - Power/Infrastructure
  - Element Management/Operations Systems
- **38 What If Scenarios**
- **Potential Alternatives Indicated**
  - Prevention/Mitigation Category
  - High/Medium/Low Cost
- **Available in NRIC Web Page**

68

Slide 69



NRIC IV Focus Group 1
Year 2000 Readiness of the Telephone Industry

Next Steps

- **Work with NCC & FCC:**
  - ICC Linkage and Information Sharing
  - USTA Investigation of Medium/Small Carrier Support

69

Appendix C: NRIC IV Focus Group 2 Subcommittee 1 Summary

NRIC

Focus Group II

Report on

Year 2K

Executive Summary

This report has been developed by a group of corporate participants under the auspices of the National Reliability and Interoperability Council. It is intended to provide telecommunications services end users with information to help manage the potential risks associated with Year 2K.

The report consists of a series of write-ups that deal with customer premise equipment (CPE) and systems that interface to the public switched telephone network (PSTN), and what owners/users of these devices/systems should know to prepare properly for Y2K.

The report consists of work done by two subcommittees. The 'Subcommittee 1' section deals with "Readiness and Testing Evaluations" for the following seven categories of devices/systems:

- PBX/Key systems
- Cell phones
- Modems
- Facsimile machines
- Devices for the disabled
- Private data networks
- Public safety answering positions

The 'Subcommittee 2' section deals with the subject of contingency planning.

The 'Readiness and Testing' reports are all formatted to provide information under the following section headings:

1.0 Description of Equipment Category – Installed Base
2.0 Information Sources
3.0 Summary of readiness Information
4.0 Assessment
5.0 Recommendations

These headings are explained further in the Introduction to the Subcommittee 1 report.

This Focus Group II report has been conducted by gathering data from a variety of sources. Input has been gathered from consultants and industry 'watchers', from manufacturer websites, and by talking with technical representatives and Y2K managers from device manufacturer and service firms.

Of the categories covered by the report several are relatively 'low risk' compared to others. Facsimile machines, for example, are unlikely to experience any problem more serious than displaying an incorrect date stamp should they experience any problem at all.

Public Safety Answering Position Systems (PSAPS) on the other hand could suffer from more consequential, and potentially serious problems. For example, all PSAP calls must record date and time stamps as they are receive d. To the extent that a PSAP system is not ready for Y2K, this time-stamping function could be impacted. Perhaps the most serious potential of all is if call overflows cause a 911 call to be blocked altogether, causing an emergency to go unattended.

Somewhere between these two extremes lies the category of Private Data Networks. Such networks are generally regarded as 'vulnerable' to Y2K problems if the appropriate evaluation and upgrades are not carried out.

Vendors of PBX/Key systems have generally prepared well for Y2K but it is still vital that equipment owners conduct a thorough evaluation of their systems to ensure that any required upgrades are identified and obtained.

Devices for the disabled and modems are not likely to incur major problems – if the proper evaluations are conducted. Recent vintage modems (i.e. those manufactured in past 2-3 years) that support 'advanced' features such as scheduling faxes are more subject to problems than older devices that simply send or receive data on command.

Regardless of the device, the key to avoiding trouble is to take responsibility for assessing the vulnerability of your devices/systems, and to take action if appropriate. Most major manufacturers have Y2K websites that contain product by product matrix listings that indicate readiness, whether testing has been done, if upgrades are required, etc. Agencies such as the National Regulatory Utility Commission (NARUC) and the National Institute of Standards and Technology (NIST – 1-800-Y2K-7557, www.Y2khelp.nist.gov) are excellent sources of information. The Federal Government also maintains two other sites that may be useful: www.y2k.link.com. and http://y2k.fts.gsa.gov/openinfo/crtree/index.asp .

The individual sites of product suppliers are referenced in each subsection of this report. Just as it is the responsibility of users to find out about their products' vulnerability, it is the manufacturers responsibility to make information easily available (e.g. on the web). With regard to contingency planning, the most effective contingency plan is one that considers all the possible consequences of equipment not performing, and developing a course of action to pursue in the event that a malfunction does occur.

As mentioned earlier, perhaps the most critical example of a contingency plan is for citizens to have local emergency phone numbers available in the event that the 911 system does not operate.

In the case of a PBX owner, the plan might include having an arrangement ahead of time regarding how to contact someone who will be able to provide technical support if a problem arises. For devices like modems and fax machines, while the consequences of a 'failure' may not be very serious, it is still worthwhile to know what you will do if a device fails. For example, if your modem is a problem, the best solution may simply be to buy a new one. Therefore, figure out which model you would buy ahead of time. If you plan on obtaining a new modem, installing it and testing well before the end of 1999 is advisable.

The general conclusions that have resulted from this effort are:

Some devices are more likely to impacted (PSAPS) than others (facsimile machines) by the Y2K event. In general, however, we can say that our investigations indicate that CPE is not likely to experience 'critical' problems if users prepare properly.

As stated in the 'Recommendation' section of each section of the report, preparation is the key. Preparation consists of several steps:

1. Take a thorough inventory of your communications devices and systems.

2. Using the inventory (i.e. manufacturer names and model numbers) contact the manufacturer to obtain information about the equipment you have – from websites, 800/888 numbers, etc.

3. Develop a plan for upgrading your communications systems – including a set of contingency actions that can be taken should something fail.

4. Obtain required (software or firmware) upgrades.

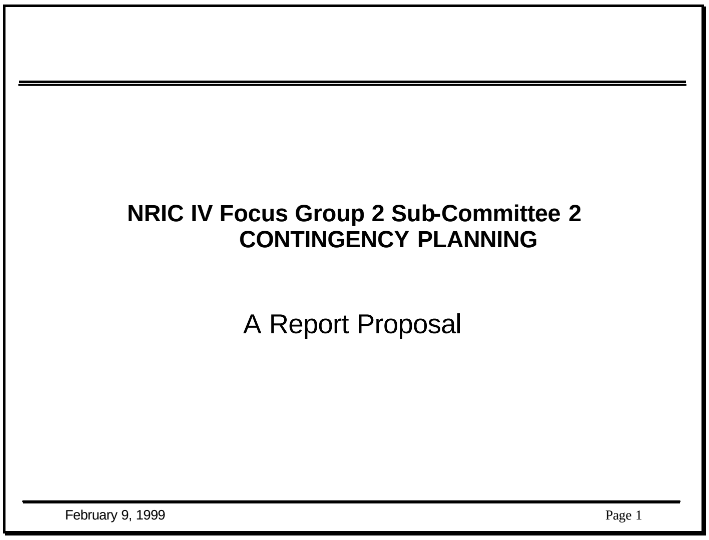
5. Test your devices/systems wherever possible; determine from your products' manufacturers if your components have been tested.

6. If you cannot find information about your product, take that as a warning sign that the manufacturer either has not done what is needed or, at best, is leaving things to chance.

If there is a general theme that we would like the reader to get from this report it is: "for CPE, Y2K is your responsibility."

Appendix D: NRIC IV Focus Group 2 Subcommittee 2 Report

Slide 1



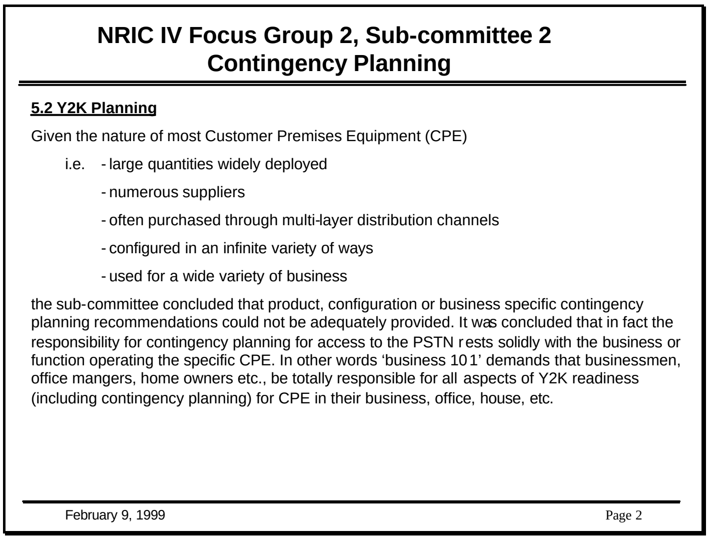
NRIC IV Focus Group 2 Sub-Committee 2
CONTINGENCY PLANNING

A Report Proposal

February 9, 1999

Page 1

Slide 2



NRIC IV Focus Group 2, Sub-committee 2
Contingency Planning

5.2 Y2K Planning

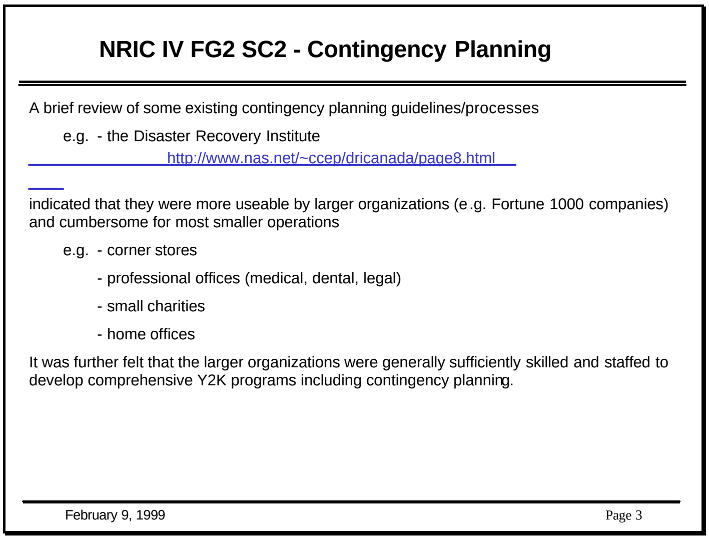
Given the nature of most Customer Premises Equipment (CPE)

i.e.
- large quantities widely deployed
- numerous suppliers
- often purchased through multi-layer distribution channels
- configured in an infinite variety of ways
- used for a wide variety of business

the sub-committee concluded that product, configuration or business specific contingency planning recommendations could not be adequately provided. It was concluded that in fact the responsibility for contingency planning for access to the PSTN rests solidly with the business or function operating the specific CPE. In other words ‘business 101’ demands that businessmen, office mangers, home owners etc., be totally responsible for all aspects of Y2K readiness (including contingency planning) for CPE in their business, office, house, etc.

February 9, 1999 Page 2

Slide 3



NRIC IV FG2 SC2 - Contingency Planning

A brief review of some existing contingency planning guidelines/processes

e.g. - the Disaster Recovery Institute

http://www.nas.net/~ccep/dricanada/page8.html

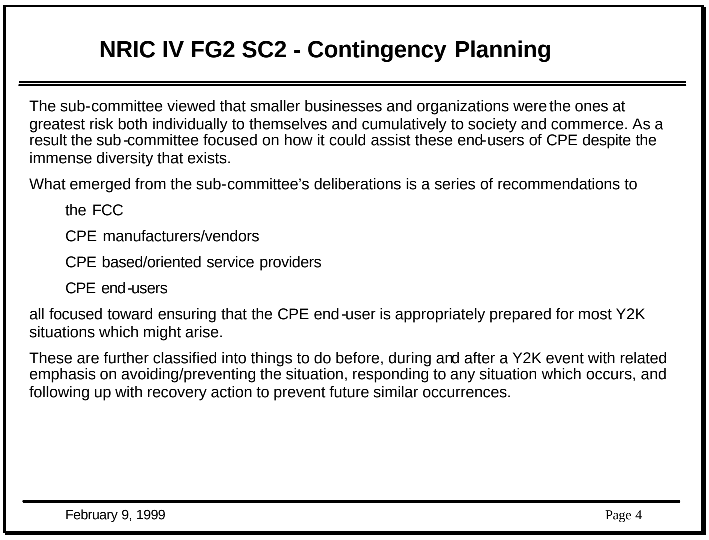
indicated that they were more useable by larger organizations (e.g. Fortune 1000 companies) and cumbersome for most smaller operations

e.g. - corner stores
- professional offices (medical, dental, legal)
- small charities
- home offices

It was further felt that the larger organizations were generally sufficiently skilled and staffed to develop comprehensive Y2K programs including contingency planning.

February 9, 1999 Page 3

Slide 4



NRIC IV FG2 SC2 - Contingency Planning

The sub-committee viewed that smaller businesses and organizations were the ones at greatest risk both individually to themselves and cumulatively to society and commerce. As a result the sub-committee focused on how it could assist these end-users of CPE despite the immense diversity that exists.

What emerged from the sub-committee's deliberations is a series of recommendations to

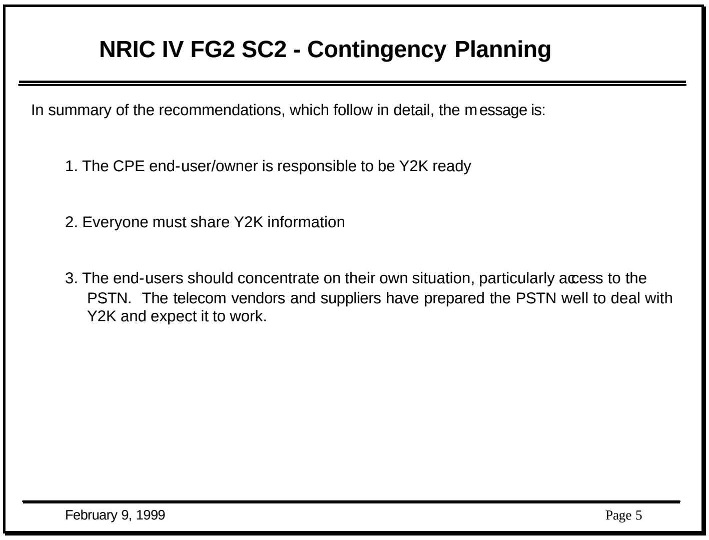
- the FCC
- CPE manufacturers/vendors
- CPE based/oriented service providers
- CPE end-users

all focused toward ensuring that the CPE end-user is appropriately prepared for most Y2K situations which might arise.

These are further classified into things to do before, during and after a Y2K event with related emphasis on avoiding/preventing the situation, responding to any situation which occurs, and following up with recovery action to prevent future similar occurrences.

February 9, 1999 Page 4

Slide 5



NRIC IV FG2 SC2 - Contingency Planning

In summary of the recommendations, which follow in detail, the message is:

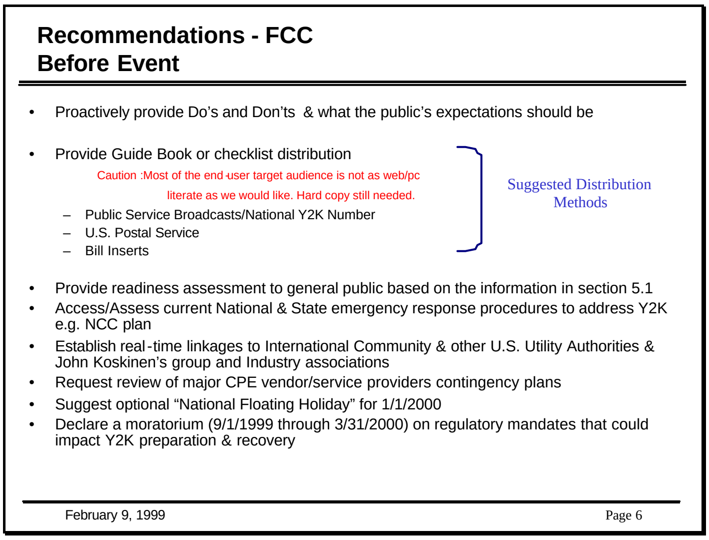
1. The CPE end-user/owner is responsible to be Y2K ready

2. Everyone must share Y2K information

3. The end-users should concentrate on their own situation, particularly access to the PSTN. The telecom vendors and suppliers have prepared the PSTN well to deal with Y2K and expect it to work.

February 9, 1999 Page 5

Slide 6



Recommendations - FCC
Before Event

- Proactively provide Do's and Don'ts & what the public's expectations should be
- Provide Guide Book or checklist distribution

  Caution :Most of the end-user target audience is not as web/pc literate as we would like. Hard copy still needed.

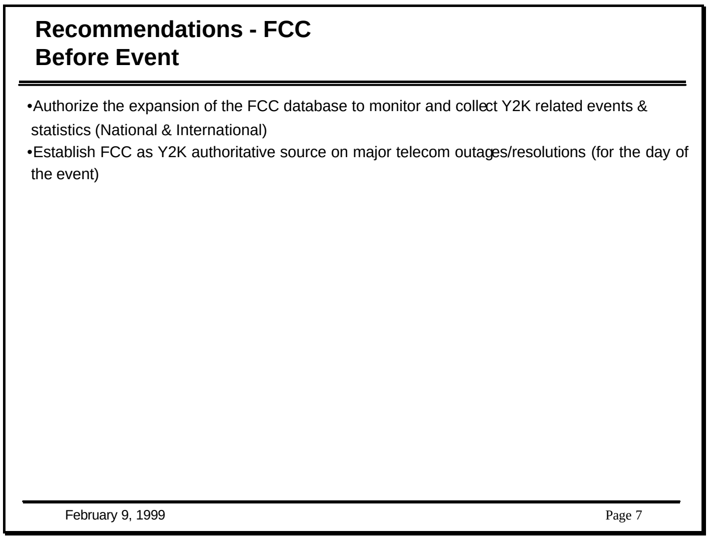
  – Public Service Broadcasts/National Y2K Number
  – U.S. Postal Service
  – Bill Inserts

Suggested Distribution Methods

- Provide readiness assessment to general public based on the information in section 5.1
- Access/Assess current National & State emergency response procedures to address Y2K e.g. NCC plan
- Establish real-time linkages to International Community & other U.S. Utility Authorities & John Koskinen's group and Industry associations
- Request review of major CPE vendor/service providers contingency plans
- Suggest optional "National Floating Holiday" for 1/1/2000
- Declare a moratorium (9/1/1999 through 3/31/2000) on regulatory mandates that could impact Y2K preparation & recovery

February 9, 1999 Page 6

Slide 7

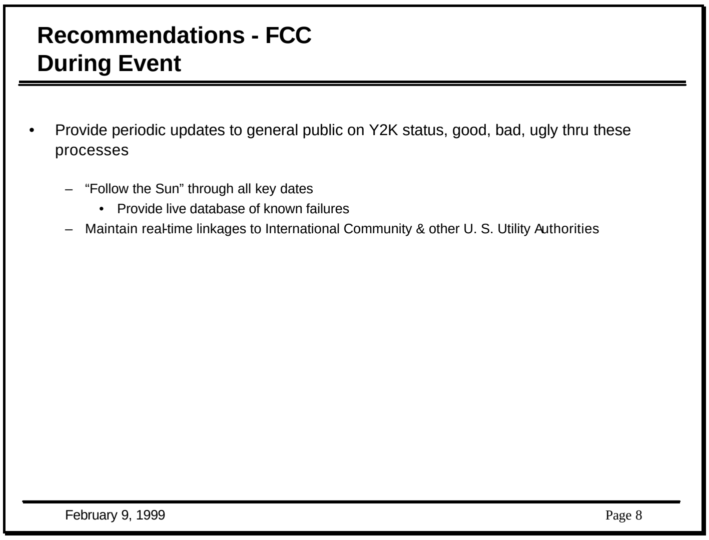


Recommendations - FCC
Before Event

- Authorize the expansion of the FCC database to monitor and collect Y2K related events & statistics (National & International)
- Establish FCC as Y2K authoritative source on major telecom outages/resolutions (for the day of the event)

February 9, 1999 Page 7

Slide 8

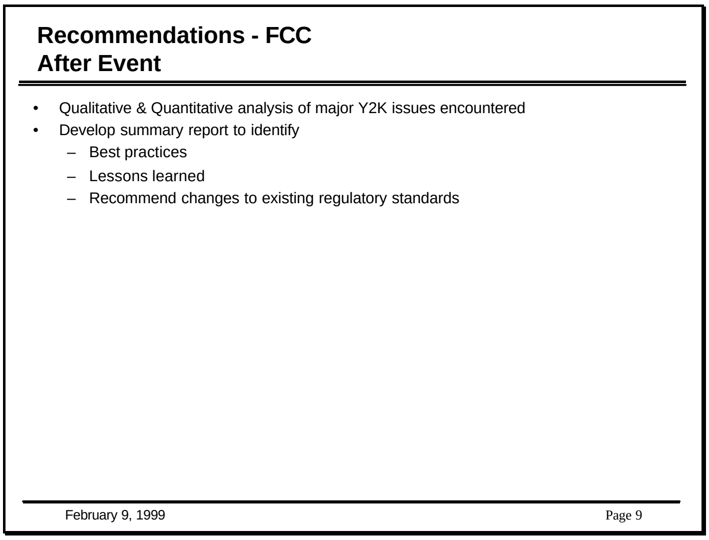


Recommendations - FCC During Event

- Provide periodic updates to general public on Y2K status, good, bad, ugly thru these processes
  - “Follow the Sun” through all key dates
    - Provide live database of known failures
  - Maintain real-time linkages to International Community & other U. S. Utility Authorities

February 9, 1999 Page 8

Slide 9

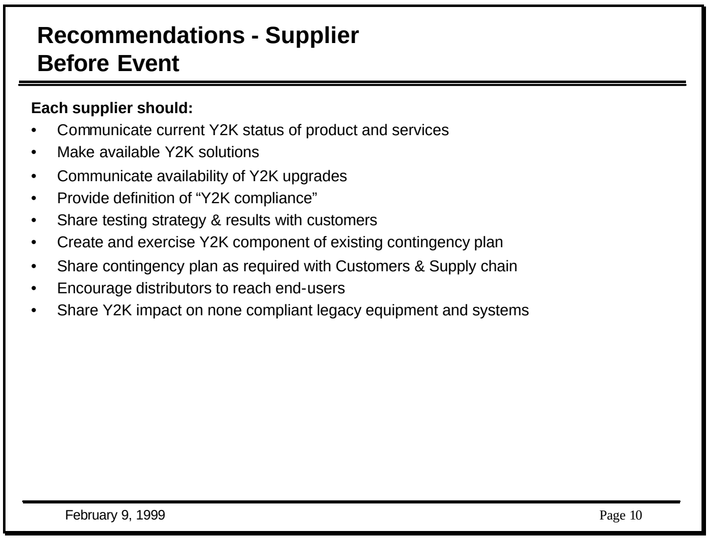


Recommendations - FCC
After Event

- Qualitative & Quantitative analysis of major Y2K issues encountered
- Develop summary report to identify
  - Best practices
  - Lessons learned
  - Recommend changes to existing regulatory standards

February 9, 1999 Page 9

Slide 10



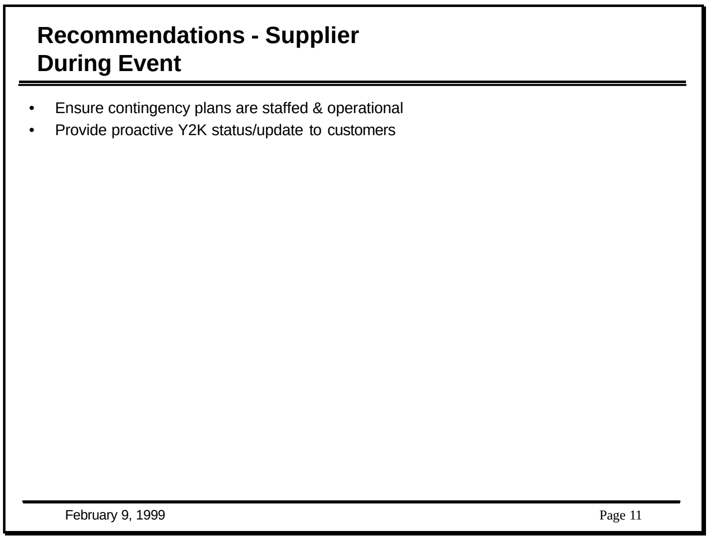
Recommendations - Supplier Before Event

Each supplier should:

- Communicate current Y2K status of product and services
- Make available Y2K solutions
- Communicate availability of Y2K upgrades
- Provide definition of “Y2K compliance”
- Share testing strategy & results with customers
- Create and exercise Y2K component of existing contingency plan
- Share contingency plan as required with Customers & Supply chain
- Encourage distributors to reach end-users
- Share Y2K impact on none compliant legacy equipment and systems

February 9, 1999 Page 10

Slide 11



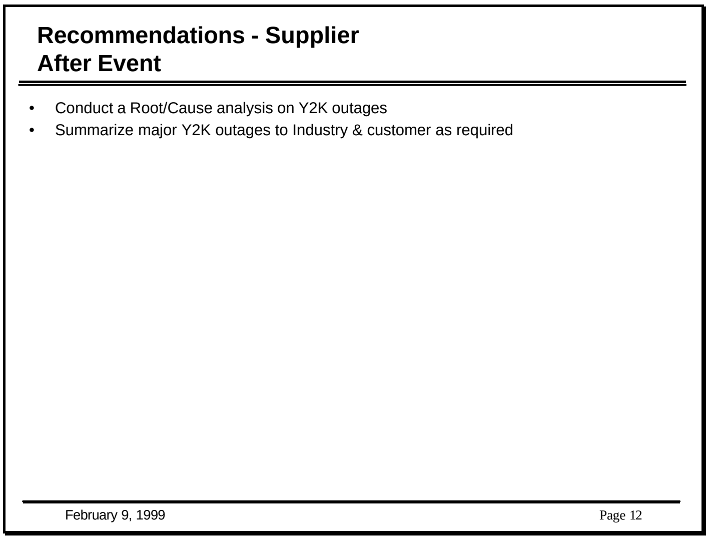
Recommendations - Supplier During Event

- Ensure contingency plans are staffed & operational
- Provide proactive Y2K status/update to customers

February 9, 1999

Page 11

Slide 12

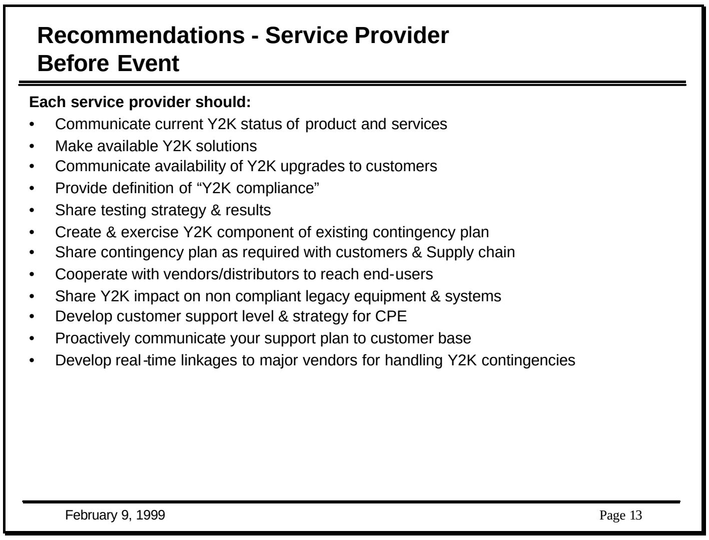


Recommendations - Supplier After Event

- Conduct a Root/Cause analysis on Y2K outages
- Summarize major Y2K outages to Industry & customer as required

February 9, 1999 Page 12

Slide 13



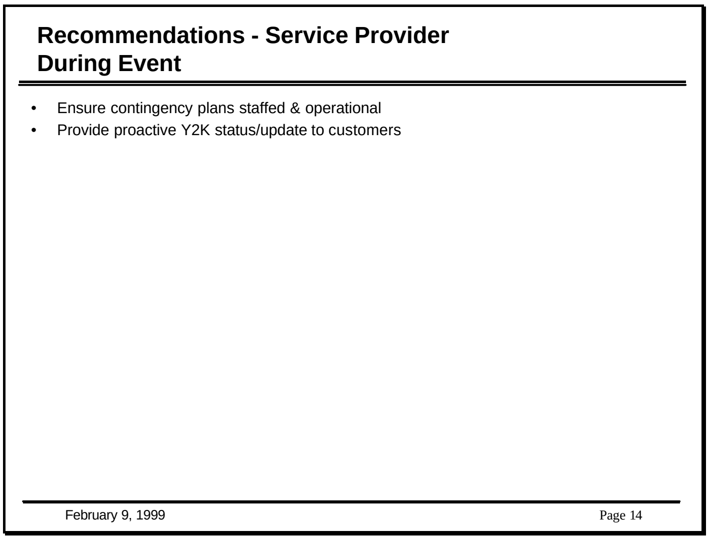
Recommendations - Service Provider Before Event

Each service provider should:

- Communicate current Y2K status of product and services
- Make available Y2K solutions
- Communicate availability of Y2K upgrades to customers
- Provide definition of "Y2K compliance"
- Share testing strategy & results
- Create & exercise Y2K component of existing contingency plan
- Share contingency plan as required with customers & Supply chain
- Cooperate with vendors/distributors to reach end-users
- Share Y2K impact on non compliant legacy equipment & systems
- Develop customer support level & strategy for CPE
- Proactively communicate your support plan to customer base
- Develop real-time linkages to major vendors for handling Y2K contingencies

February 9, 1999 Page 13

Slide 14



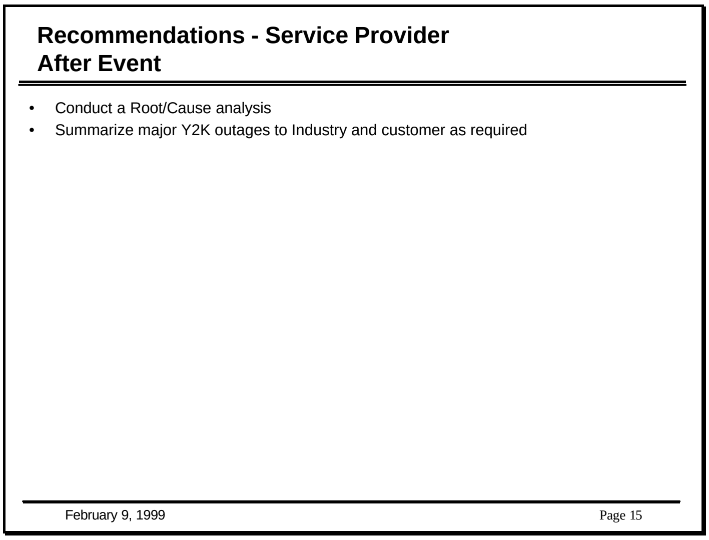
Recommendations - Service Provider During Event

- Ensure contingency plans staffed & operational
- Provide proactive Y2K status/update to customers

February 9, 1999

Page 14

Slide 15



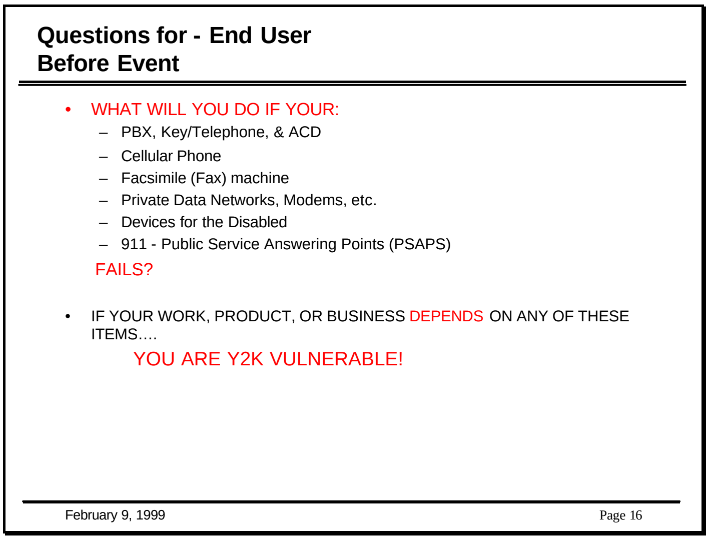
Recommendations - Service Provider After Event

- Conduct a Root/Cause analysis
- Summarize major Y2K outages to Industry and customer as required

February 9, 1999

Page 15

Slide 16



Questions for - End User Before Event

- WHAT WILL YOU DO IF YOUR:
  - PBX, Key/Telephone, & ACD
  - Cellular Phone
  - Facsimile (Fax) machine
  - Private Data Networks, Modems, etc.
  - Devices for the Disabled
  - 911 - Public Service Answering Points (PSAPS)

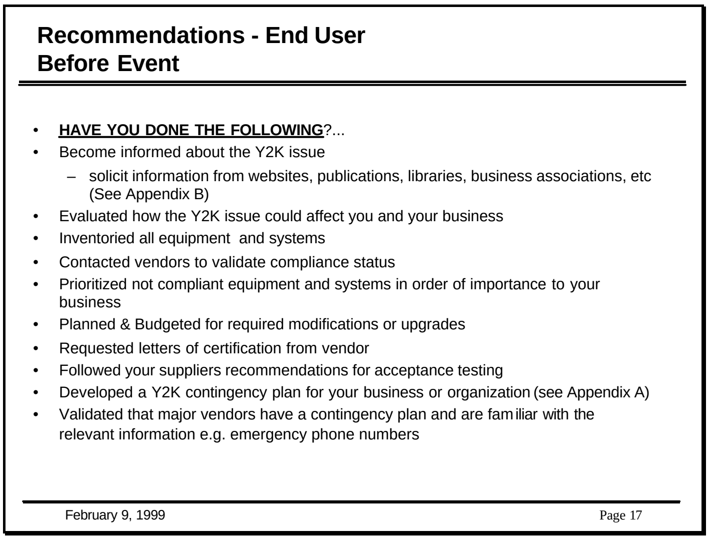
  FAILS?

- IF YOUR WORK, PRODUCT, OR BUSINESS DEPENDS ON ANY OF THESE ITEMS….

  YOU ARE Y2K VULNERABLE!

February 9, 1999 Page 16

Slide 17



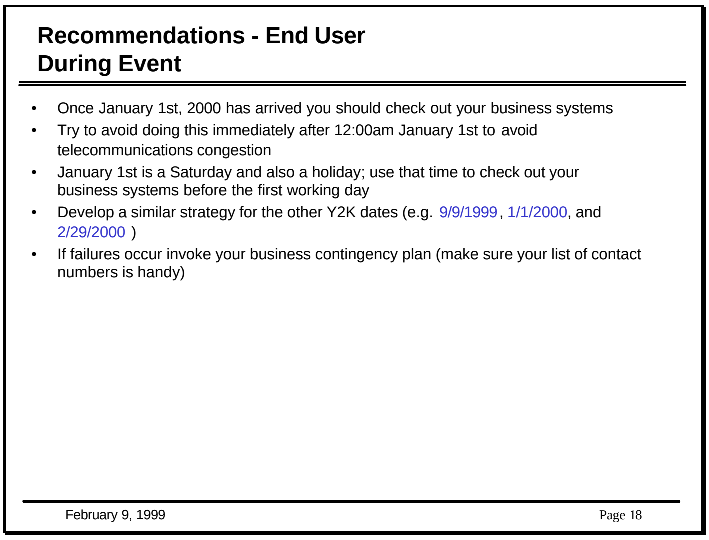
Recommendations - End User
Before Event

- **HAVE YOU DONE THE FOLLOWING**?...
- Become informed about the Y2K issue
  - solicit information from websites, publications, libraries, business associations, etc (See Appendix B)
- Evaluated how the Y2K issue could affect you and your business
- Inventoried all equipment and systems
- Contacted vendors to validate compliance status
- Prioritized not compliant equipment and systems in order of importance to your business
- Planned & Budgeted for required modifications or upgrades
- Requested letters of certification from vendor
- Followed your suppliers recommendations for acceptance testing
- Developed a Y2K contingency plan for your business or organization (see Appendix A)
- Validated that major vendors have a contingency plan and are familiar with the relevant information e.g. emergency phone numbers

February 9, 1999

Page 17

Slide 18



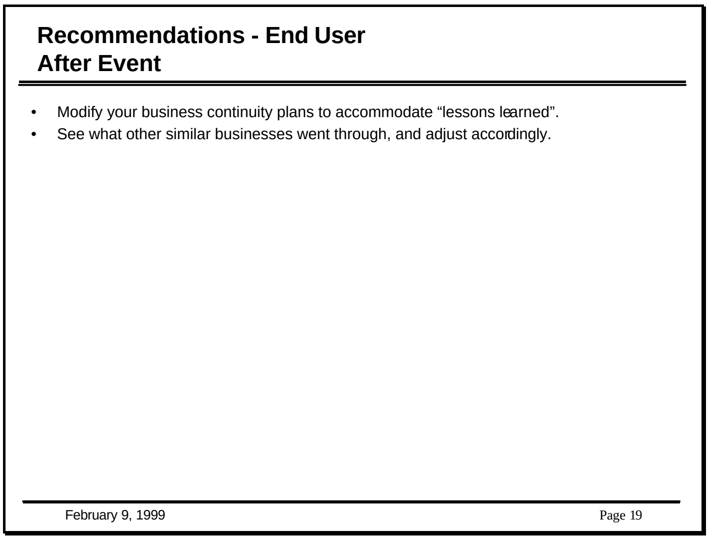
Recommendations - End User During Event

- Once January 1st, 2000 has arrived you should check out your business systems
- Try to avoid doing this immediately after 12:00am January 1st to avoid telecommunications congestion
- January 1st is a Saturday and also a holiday; use that time to check out your business systems before the first working day
- Develop a similar strategy for the other Y2K dates (e.g. 9/9/1999, 1/1/2000, and 2/29/2000)
- If failures occur invoke your business contingency plan (make sure your list of contact numbers is handy)

February 9, 1999

Page 18

Slide 19



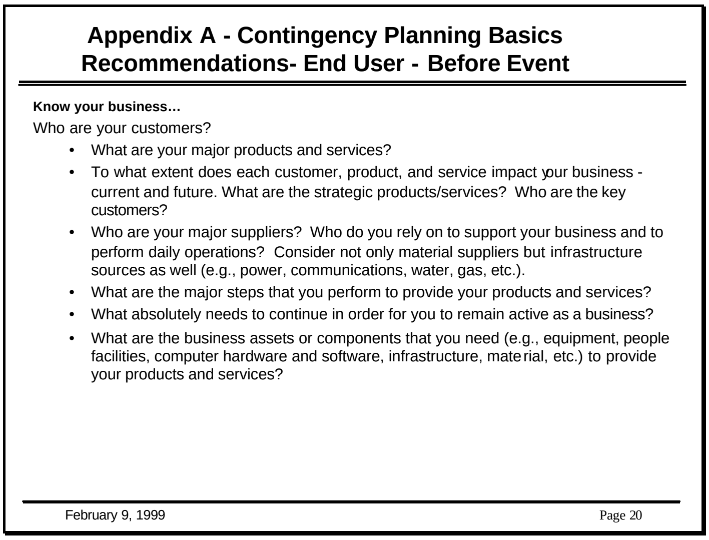
Recommendations - End User After Event

- Modify your business continuity plans to accommodate “lessons learned”.
- See what other similar businesses went through, and adjust accordingly.

February 9, 1999

Page 19

Slide 20



Appendix A - Contingency Planning Basics
Recommendations- End User - Before Event

Know your business…

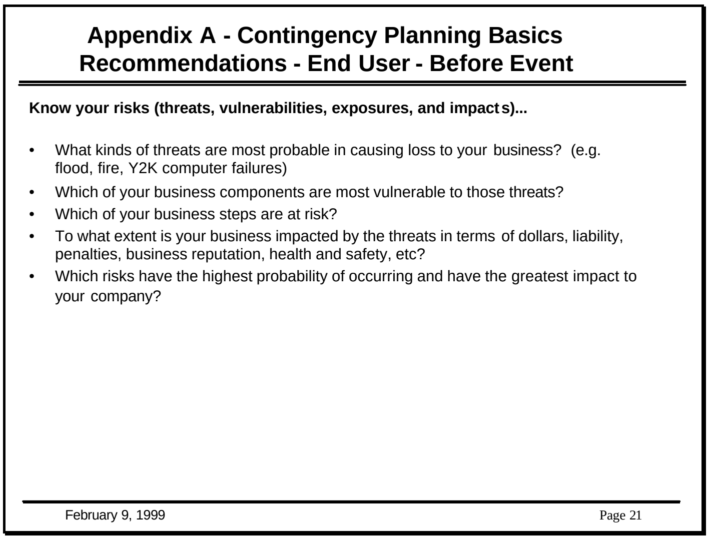
Who are your customers?

- What are your major products and services?
- To what extent does each customer, product, and service impact your business - current and future. What are the strategic products/services? Who are the key customers?
- Who are your major suppliers? Who do you rely on to support your business and to perform daily operations? Consider not only material suppliers but infrastructure sources as well (e.g., power, communications, water, gas, etc.).
- What are the major steps that you perform to provide your products and services?
- What absolutely needs to continue in order for you to remain active as a business?
- What are the business assets or components that you need (e.g., equipment, people facilities, computer hardware and software, infrastructure, material, etc.) to provide your products and services?

February 9, 1999

Page 20

Slide 21



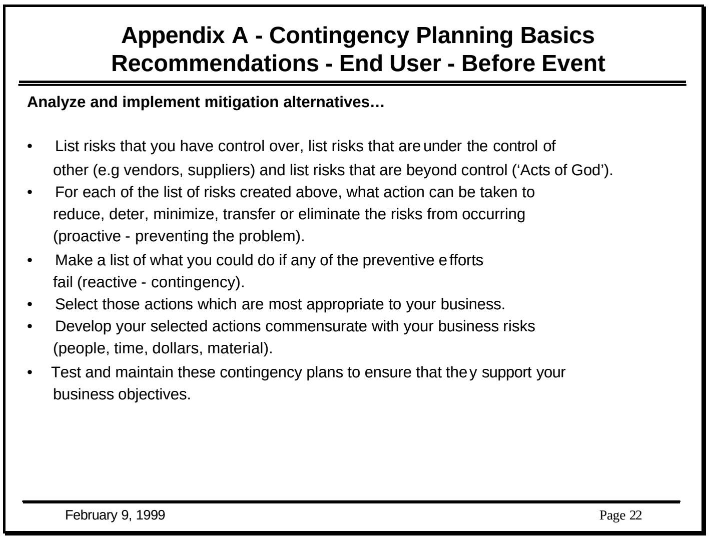
Appendix A - Contingency Planning Basics
Recommendations - End User - Before Event

Know your risks (threats, vulnerabilities, exposures, and impacts)...

- What kinds of threats are most probable in causing loss to your business? (e.g. flood, fire, Y2K computer failures)
- Which of your business components are most vulnerable to those threats?
- Which of your business steps are at risk?
- To what extent is your business impacted by the threats in terms of dollars, liability, penalties, business reputation, health and safety, etc?
- Which risks have the highest probability of occurring and have the greatest impact to your company?

February 9, 1999 Page 21

Slide 22



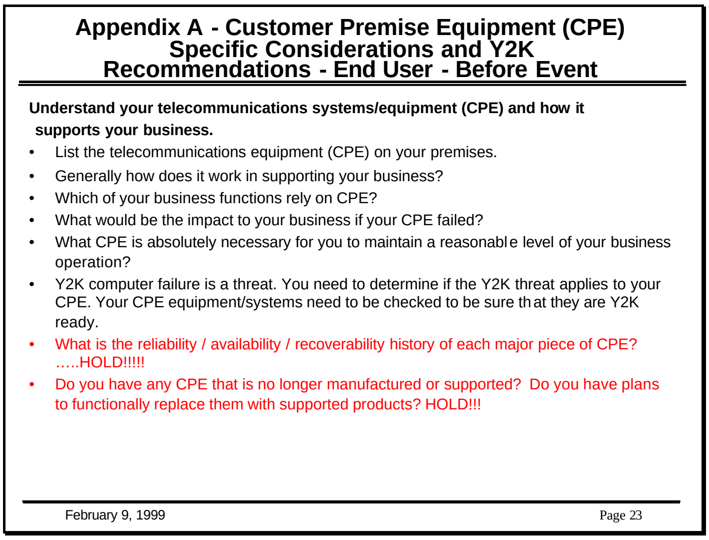
Appendix A - Contingency Planning Basics
Recommendations - End User - Before Event

Analyze and implement mitigation alternatives…

- List risks that you have control over, list risks that are under the control of other (e.g vendors, suppliers) and list risks that are beyond control ('Acts of God').
- For each of the list of risks created above, what action can be taken to reduce, deter, minimize, transfer or eliminate the risks from occurring (proactive - preventing the problem).
- Make a list of what you could do if any of the preventive efforts fail (reactive - contingency).
- Select those actions which are most appropriate to your business.
- Develop your selected actions commensurate with your business risks (people, time, dollars, material).
- Test and maintain these contingency plans to ensure that they support your business objectives.

February 9, 1999 Page 22

Slide 23



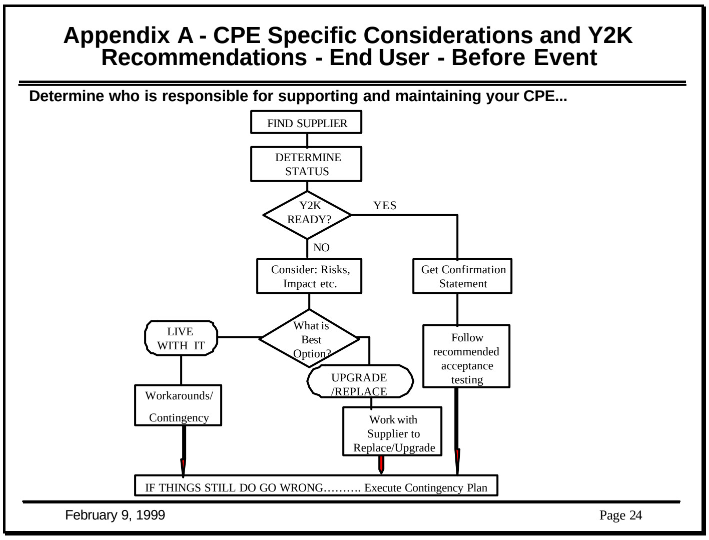
Appendix A - Customer Premise Equipment (CPE) Specific Considerations and Y2K Recommendations - End User - Before Event

Understand your telecommunications systems/equipment (CPE) and how it supports your business.

- List the telecommunications equipment (CPE) on your premises.
- Generally how does it work in supporting your business?
- Which of your business functions rely on CPE?
- What would be the impact to your business if your CPE failed?
- What CPE is absolutely necessary for you to maintain a reasonable level of your business operation?
- Y2K computer failure is a threat. You need to determine if the Y2K threat applies to your CPE. Your CPE equipment/systems need to be checked to be sure that they are Y2K ready.
- What is the reliability / availability / recoverability history of each major piece of CPE? …..HOLD!!!!!
- Do you have any CPE that is no longer manufactured or supported? Do you have plans to functionally replace them with supported products? HOLD!!!

February 9, 1999 Page 23

Slide 24



Appendix A - CPE Specific Considerations and Y2K Recommendations - End User - Before Event

Determine who is responsible for supporting and maintaining your CPE...

FIND SUPPLIER

DETERMINE STATUS

Y2K READY?

YES

NO

Consider: Risks, Impact etc.

Get Confirmation Statement

LIVE WITH IT

What is Best Option?

Follow recommended acceptance testing

UPGRADE /REPLACE

Workarounds/ Contingency

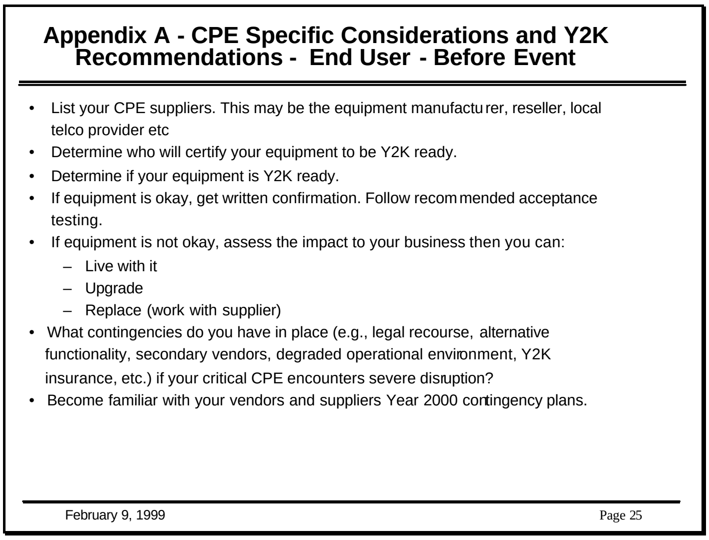
Work with Supplier to Replace/Upgrade

IF THINGS STILL DO GO WRONG………. Execute Contingency Plan

February 9, 1999

Page 24

Slide 25

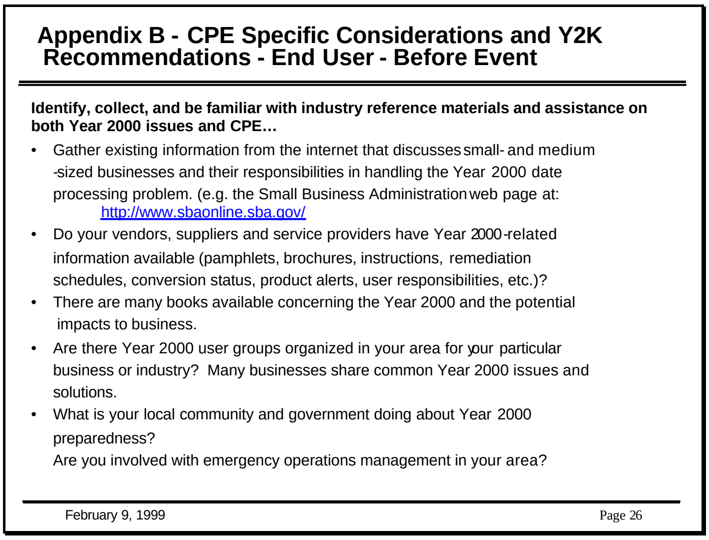


Appendix A - CPE Specific Considerations and Y2K Recommendations - End User - Before Event

- List your CPE suppliers. This may be the equipment manufacturer, reseller, local telco provider etc
- Determine who will certify your equipment to be Y2K ready.
- Determine if your equipment is Y2K ready.
- If equipment is okay, get written confirmation. Follow recommended acceptance testing.
- If equipment is not okay, assess the impact to your business then you can:
  - Live with it
  - Upgrade
  - Replace (work with supplier)
- What contingencies do you have in place (e.g., legal recourse, alternative functionality, secondary vendors, degraded operational environment, Y2K insurance, etc.) if your critical CPE encounters severe disruption?
- Become familiar with your vendors and suppliers Year 2000 contingency plans.

February 9, 1999 Page 25

Slide 26



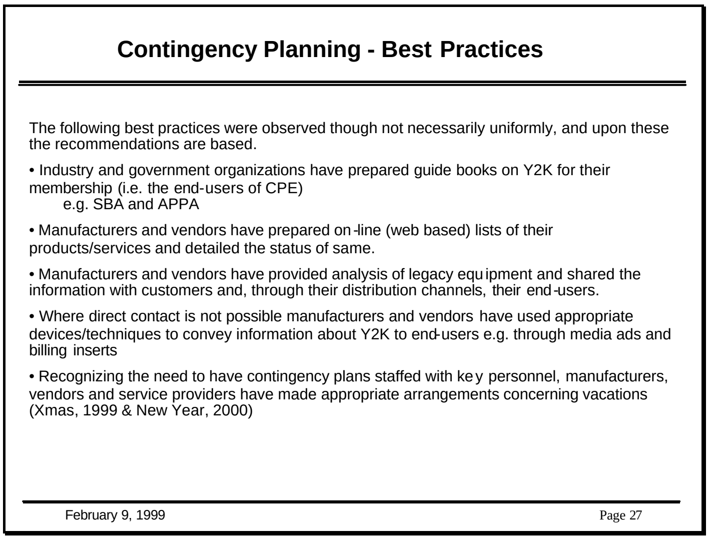
Appendix B - CPE Specific Considerations and Y2K Recommendations - End User - Before Event

Identify, collect, and be familiar with industry reference materials and assistance on both Year 2000 issues and CPE…

- Gather existing information from the internet that discusses small- and medium -sized businesses and their responsibilities in handling the Year 2000 date processing problem. (e.g. the Small Business Administration web page at: http://www.sbaonline.sba.gov/
- Do your vendors, suppliers and service providers have Year 2000-related information available (pamphlets, brochures, instructions, remediation schedules, conversion status, product alerts, user responsibilities, etc.)?
- There are many books available concerning the Year 2000 and the potential impacts to business.
- Are there Year 2000 user groups organized in your area for your particular business or industry? Many businesses share common Year 2000 issues and solutions.
- What is your local community and government doing about Year 2000 preparedness?
  Are you involved with emergency operations management in your area?

February 9, 1999 Page 26

Slide 27



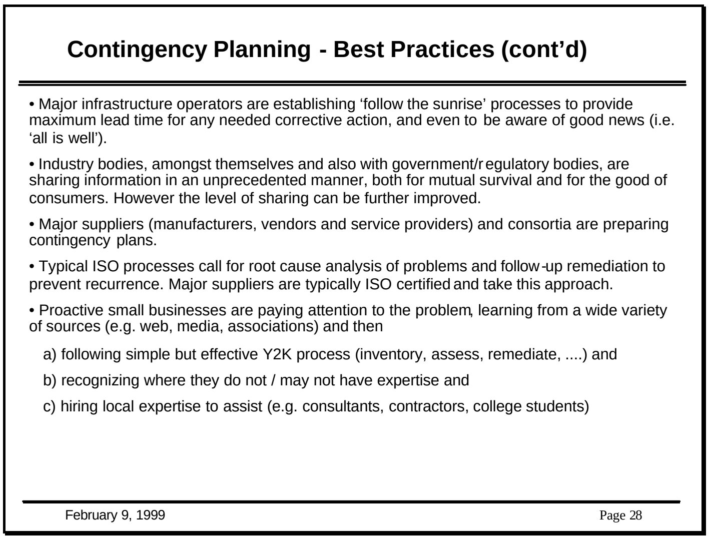
Contingency Planning - Best Practices

The following best practices were observed though not necessarily uniformly, and upon these the recommendations are based.

- Industry and government organizations have prepared guide books on Y2K for their membership (i.e. the end-users of CPE)
  e.g. SBA and APPA
- Manufacturers and vendors have prepared on-line (web based) lists of their products/services and detailed the status of same.
- Manufacturers and vendors have provided analysis of legacy equipment and shared the information with customers and, through their distribution channels, their end-users.
- Where direct contact is not possible manufacturers and vendors have used appropriate devices/techniques to convey information about Y2K to end-users e.g. through media ads and billing inserts
- Recognizing the need to have contingency plans staffed with key personnel, manufacturers, vendors and service providers have made appropriate arrangements concerning vacations (Xmas, 1999 & New Year, 2000)

February 9, 1999 Page 27

Slide 28



Contingency Planning - Best Practices (cont'd)

- Major infrastructure operators are establishing 'follow the sunrise' processes to provide maximum lead time for any needed corrective action, and even to be aware of good news (i.e. 'all is well').
- Industry bodies, amongst themselves and also with government/regulatory bodies, are sharing information in an unprecedented manner, both for mutual survival and for the good of consumers. However the level of sharing can be further improved.
- Major suppliers (manufacturers, vendors and service providers) and consortia are preparing contingency plans.
- Typical ISO processes call for root cause analysis of problems and follow-up remediation to prevent recurrence. Major suppliers are typically ISO certified and take this approach.
- Proactive small businesses are paying attention to the problem, learning from a wide variety of sources (e.g. web, media, associations) and then

  a) following simple but effective Y2K process (inventory, assess, remediate, ...) and

  b) recognizing where they do not / may not have expertise and

  c) hiring local expertise to assist (e.g. consultants, contractors, college students)

February 9, 1999 Page 28

Appendix E: NRIC IV Focus Group 3 Subcommittee 1 Report

Executive Summary

Background

The Best Practice Team was originally convened under the auspices of the Network Reliability Council (NRC II) in the Fall of 1994, to determine the level of awareness and implementation of Best Practices and recommendations from NRC I, and whether companies were actually implementing them. In June 1993, the Federal Communications Commission's (FCC) Network Reliability Council (NRC I) had published "Network Reliability: A Report to the Nation." This document contained technical papers written by the NRC Focus Teams. The focus teams, composed of contributors from both inside and outside the telecommunications industry, were established to conduct in-depth studies of seven network reliability areas that were considered to be of highest priority based on historical data, namely:

- Fiber Cable Systems
- Signaling Network Systems
- Switching Systems
- Digital Cross-Connect Systems
- Power Systems
- E-911 Systems (Focus Group IV)
- Fire Prevention.

The NRC encouraged the industry to study and assess the applicability of recommendations contained in the technical papers for implementation in their companies, with the following caveat: *"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 will sustain and continuously improve network reliability."* The compendium of technical papers became known as the "Purple Book" and the recommendations therein became known as Best Practices. Note that the original focus teams made recommendations and identified Best Practices, already in use by individual companies, for consideration by the rest of the industry. The findings of the NRC were shared with the industry at a national symposium that was held in June of 1993. There were very few cases where the identified Best Practices were actually endorsed or recommended by the focus teams.

The NRC (NRC II) established new Task Groups when it was formed. The Network Reliability Performance Committee (NRPC) was formed by the Alliance for Telecommunications Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC) to fulfill the mission of the NRC's Task Group I to address network reliability performance. The NRPC chartered the Best Practice Team (BPT) to address the following issues assigned to it by the NRC:

1. Recommend and implement relevant measures of the industry's implementation of Best Practices.

2. Determine if and to what extent industry is implementing applicable Best Practices.

3. Evaluate the effectiveness of applicable Best Practice for avoiding or mitigating service outages.

4. Determine the cost/value of applicable Best Practices.

5. Determine if there are additional or new Best Practices that should be added to the current set being utilized in industry today.

The end result of the work of the Best Practice team was a set of Best Practices again, arranged into the original NRC Focus Areas, which was published in *Network Reliability: The Path Forward*, which came to be known as the “Red Book”.

Current Situation

In 1998, the Network Reliability and Interoperability Council IV (NRIC IV) Focus Group 3 established the current Best Practice Team to reassess implementation of these Best Practices, determine applicability to new industry segments and entrants and identify any new Best Practices. It was further recommended that the Best Practice Team focus its attention on Power, Facilities, and Procedural best practices based on the outage trends identified by the Network Reliability Steering Committee (NRSC). The Best Practice Team also focused on Essential Services as a result of concerns expressed by the FCC, even though the NRSC analyses have not identified any negative trend in E911 outages this revision has incorporated all Best Practices, including those identified in NRC II and III as well as other NRSC activities subsequent to the earlier Best Practice Team's review.

The Best Practice Team has consolidated the original NRC Focus Areas to better relate to the current industry environment and segments and eliminate duplication and redundancy of Best Practices in the original focus areas. The Best Practice Team also decided that it was time to eliminate the references back to the original Purple Book, which is not available in electronic format. Current players in the industry may have no history with the book. It was agreed that a complete and self contained set of best practices, without references to an outdated book or study, should be developed for ongoing use. The Team further agreed to reword the best practices to make them more generic and so, applicable to new industry segments and entrants. The Team also expanded the Power Best Practices. The original list had 27 Power Best Practices that were actually groupings of subsets of Best Practices. The new list includes 84 Power Best Practices.

To evaluate the current status of Best Practices in the industry, service providers and suppliers were surveyed on Best Practice implementation, effectiveness and cost to implement. As expected, the majority of the traditional service providers and suppliers responded however, there were limited responses from the new industry players. Local exchange carriers that responded serve approximately 95% of the nation's access lines. Major long distance carriers and equipment suppliers responded as well, although we have no figures to support market share covered by the responses. Overall, the responses indicate that there is a continuing high level of implementation of Best Practices among these service providers and suppliers. The survey responses for each Best Practice were compiled and reviewed which resulted in some more "fine tuning", deletions, and consolidation of the Best Practices.

The Team also reviewed outage trends and actual outage reports for any Best Practice implications. This review confirmed the applicability of the existing best practices and did not turn up any new Best Practices. The adverse trends in Power and Procedural outages, coupled with the survey implementation results, suggest that carriers may "have a policy" about use of Best Practices however, the frequency of outages suggests that Best Practices are not being consistently applied.

The Team also reviewed the *"* ***Procedural Outage Reduction: Addressing the Human Part*** *"* prepared by the NRSC's Procedural Error Team and added some new Best

Practices to the list based on the recommendations of that report. The report also confirmed the importance of following many of the existing Best Practices. The work of the NRSC Facilities Solutions Team was also reviewed and the entire set of their Best Practices are included in the Team's new set of Best Practices.

In August 1999, the NRSC reviewed data for the most recent study year, 7/1/98 through 6/30/99, which reflected a continuing serious problem with Power outages. The NRSC asked the Best Practice Team to study this problem and make some recommendations. The Team then reviewed the Power outages and the associated Best Practices for every power outage during that period. The Best Practice Team concluded that increased attention to Best Practices relating to Installation activities is warranted, and no new Best Practices were identified.

The final recommendation of the Best Practice Team is for companies (including new entrants) to implement the new set of Best Practices where applicable, and ensure that they are actually followed. The Team further recommends that companies include Best Practice considerations and analysis in their ongoing FCC outage reporting.

Background

Scope Statement

Report on the reliability of public telecommunications network services in the United States; determine whether "best practices" previously recommended should be modified or supplemented; and develop a proposal for future consideration relative to extending these best practices to other industry segments not presently included in current practices.

This subcommittee should focus on Facility and Power related outages and those caused by procedural errors.

Deliverables and Work Plan

- Identify Team Members
- Set meeting/conference call schedule
- Establish communications vehicle/web site

- Review of Current Documents
  - Update Best Practice List to include new/additional Best Practices Identified by NRC II, NRIC III and NRSC activity
  - Review Best Practices - Focus of review:
  - "Procedural" Best Practices for all focus areas
  - All Best Practices in Power, E911 and Facilities focus areas
  - Update/revise all Best Practices to be more generic and applicable to new entrants and new technology deployment
  - Review Outage Reports for examples of Best Practice effectiveness and areas where Best Practices are needed or lacking
  - Identify other potential sources for best practices not currently documented via NRIC/NRSC

- Data Collection
  - Develop and issue data collection questionnaire
    - Solicit data on implementation and effectiveness (target – incumbent/traditional car and suppliers)
  - Analyze responses and develop report
  - Share data with new entrants and suppliers
- Develop Final Report
  - Assemble a new complete set of Best Practices
  - Agree on Final Recommendations

Team Members

PJ Aduskevicz	AT&T	J.R. Lofstedt	U S WEST
Ray Albers	Bell Atlantic	Norb Lucash	USTA
Ray Bonelli	Lucent	Anil Macwan	Lucent
Rick Canaday	AT&T	Spilios Makris	Telcordia
Wayne Chiles	Bell Atlantic	Henry Malec	3Com
Judy Glatz	AT&T	Clyde Miller	Nortel
Glenn Grotefeld	Motorola	Irv Picus	NTIA
Rick Harrison	Telcordia	Michael Posch	Ameritech
John Healy	Telcordia	Karl Rauscher	Lucent
James Keown	SBC	Richard Round	GTE
Scott Taylor	BellSouth	Jim Kerr	NCS
Whitey Thayer	FCC Bill Klein	ATIS	
	Jerry Usry	Sprint	

Data Collection and Analysis Methodology

To fulfill its mission, the Best Practice Team determined that it required information from traditional telecommunications service providers and from suppliers regarding their usage of the Best Practices. Accordingly, the Best Practices Team developed two questionnaires, one for service providers and one for suppliers, in order to obtain information about the following:

- The extent of implementation of the Best Practices,
- Ratings of their effectiveness,
- The relative cost of implementation.

The Network Reliability and Interoperability Council IV (NRIC IV) Focus Group 3 designated Telcordia Technologies as the central point for requesting, collecting, compiling, and aggregating data for both teams including the Best Practices Team. All data collected by Telcordia was treated as proprietary information. Specific references to individual respondents were removed and the Best Practices Team was only shown aggregated results.

The Network Reliability Steering Team has noted that there has been an increasing trend in the number of FCC reportable outages for power outages, for procedural outages and for facility outages. In addition, the FCC has continued to desire information on E9-1-1 outages. As a result, the first questionnaire for service providers covered Best Practices on power outages, procedural outages, and E9-1-1 outages. The second questionnaire for suppliers had a similar type of coverage.

An independent survey of Best Practices for facility outages was already underway by the Facilities Solution Team. The Best Practices Team used results from this independent survey in lieu of sending out an additional, superfluous questionnaire. The remainder of this section describes the questionnaires and the process used to administer them and summarizes the response rates from the industry.

Questionnaire Description

The service provider questionnaire and the supplier questionnaire had the same form. They differed in the Best Practices that were covered. A copy of the questionnaire for service providers excluding facility Best Practices and the questionnaire for suppliers are in Appendix A and B, respectively. A copy of the questionnaire for service providers covering facility Best Practices is in Appendix C.

The questionnaires were in spreadsheet form and were aimed at collecting statistical information on the level of implementation of the recommendations, an assessment of their effectiveness and the costs to implement the recommendations. The questionnaires were distributed electronically. The companies were asked to provide their responses in electronic form, if possible, and most did so. The supplier request had a shorter list of practices and the questionnaire was also provided electronically.

At the top of each questionnaire, there was a place to enter the company's name and the name and telephone number of a contact person in case there were any questions about a company's responses.

The first column of the spreadsheet contained an identifying number for each recommendation. Column B gave a summary statement of the recommendation. For the power Best Practices, many of the Best Practices that were originally contained in the document *Network Reliability: A Report to the Nation* were split into several Best Practices. For the procedural Best Practices, the same Best Practice could be found in more than one Focus Area of the documents *Network Reliability: A Report to the Nation* or *Network Reliability: The Path Forward*. For example, the same Best Practice could be found under Signaling Systems and under DCS. The Best Practice Team genericized each Best Practice and eliminated any duplication. For the Emergency Services Best Practices, the Best Practices Team decided to include nearly all the verbiage from the original sources. Column C provided a source(s) for the recommendation

Columns D through F were filled in by the respondents. Column D dealt with a company's implementation of each Best Practice. A company was asked to indicate whether the Best Practice was implemented (E) Everywhere, (NE) Nearly Everywhere, (C) In Critical Places Only, (F) In Few Places (Very Limited Implementation), or (N) Nowhere.

In column E, companies were asked to rate the effectiveness of the recommendation in enhancing network reliability and preventing or reducing outages. A scale of 1 to 5 was used with the following interpretation:

5 The practice is definitely effective in preventing or reducing outages based, for example, on quantifiable measurements and experience.

4 Based on intuitive opinions or anecdotal evidence, the practice is effective in preventing or reducing outages.

3 The practice is somewhat, or moderately, effective in preventing or reducing outages.

2 The practice is only slightly effective in preventing or reducing outages.

1 The recommendation is basically ineffective in preventing or reducing outages.

The respondent could enter 0 in Column E to indicate that the company did not know the effectiveness of the practice.

Column F asked each company to rate the cost to implement a practice, relative to the other Best Practices. The choices were Very Low (VL), Low (L), Moderate (M), High (H), and Very High (VH). A Very Low rating suggested that there were essentially no additional cost above the normal costs of doing business for implementing that Best

Practice. A Very High rating suggested major capital or operating expenditures would be required.

The Supplier Best Practice Questionnaire was identical in structure to the Service Provider Best Practice Questionnaire (see Appendix B). The Best Practice Questionnaire for Facilities also asked the respondent to rate the effectiveness, cost and implementation of the Best Practice. It also contained several additional questions such as whether the Best Practice was obsolete or whether a Best Practice was too general (see Appendix C).

Data Collection Process

Since the original Best practices were aimed at major telecommunications service providers and suppliers, the Best Practices questionnaires were sent to major telecommunications carriers and to major equipment suppliers. All questionnaires were returned via e-mail, fax or regular mail to Telcordia Technologies.

The questionnaires were sent to the service providers on April 30 and May 5, 1999. The original due-date for responses was May 15, 1999. However this date was extended to July 10, 1999, to include as many responses as possible. One questionnaire was returned on September 7. Of the 14 companies which received questionnaires, 7 responded.

Most of the supplier questionnaires were sent out on May 5 and May 11. Several were sent out after May 11 as contact names were identified. Of the 11 companies which received questionnaires, 5 responded.

The facility questionnaire was sent to the RBOCs and interexchange carriers in July, 1998. The original due-date for responses was August 15, 1998. By December 18, 1998, every company had responded. There were a total of ten responses.

The final tally of returned questionnaires was as follows:

Industry Segment	**Number of Responses**
Service Providers	7
Suppliers	5
Service Providers - Facilities	10
Total	**22**

Data Aggregation and Analysis Process

For each questionnaire, the initial aggregation was a table with average ratings of each of the Best practices. In addition, graphs of the average level of implementation, effectiveness and cost were developed. These graphs presented one variable at a time.

The team decided that a composite graph which simultaneously exhibits the effectiveness, the cost, and the level of implementation was the most useful in analyzing the Best Practices. These graphs were used to draw conclusions about Best Practices. These graphs are presented in Appendix D.

Findings: Observations and Recommendations

Observations

Overall

Overall implementation of Best Practices by traditional service providers and suppliers remains high. The review of outage reports and survey responses confirm the applicability of most of the original Best Practices and has not turned up any new Best Practices. Unless otherwise stated the reference numbers for the Best Practices are their old reference numbers.

Power (PW)

The following observations were made as a result of the Best Practice by Best Practice review of survey responses.

- All existing best practices have been rated as effective
- Review of power outage reports (past 2 Years) supports the need for following existing best practices
- Outage index (customer impact) reflects effectiveness of power best practices in mitigating outage impact
- PW01 (human factors) was reworded to make it more actionable. Also - Human Factors have been considered and incorporated in newer power equipment however, power equipment has a long life cycle and is typically upgraded or replaced based on the need for more power and not because of new technology or improved human factors features.
- Six Power BPs have been identified as having Limited Application
- PW27 (AC Tap Boxes) was deleted as a BP
- PW44 (multiple smaller plants closer to the load) was deleted as it was redundant with PW33
- BPs (8) originally endorsed based on Hurricane Andrew post mortem were found to either: have Limited Application; be redundant with other BPs; conflict with other BPs; or not be BPs at all.
- PW10 (onsite/re-supply plan fuel supply) was found to be a real winner

Analysis of 7/1/98 – 6/30/99 Power Outages

22 Outages total

12 - Root Cause Commercial/Backup Power Failure

10 Root Cause Procedural

8 Sub Cause Standby Generator

Best Practice Team Findings:

- 16 Outages with Best Practice implications

PW BPs applicable to outages	**Number of outages**

PW45	3 Outages
PW69-71	7 Outages
PR03	7 Outages
PW57, 58	2 Outages
PW51, 52, 56	2 Outages

- PW69-71 (new PW66-68) & PR03 All relate to MOPs and Installation Guidelines
- PW69(new PW66) – Service Providers should have documented installation guidelines
- PW70(new PW67) – Service Providers should clearly communicate their installation guidelines to all involved parties
- PW71(new PW68) - On-site installation acceptance should include a quality review of conformance to the company's and vendor's guidelines
- PR03 - MOPs and Acceptance/Verification Check-off Sheets for Hardware and Software Growth/Change Activities …
- All of the above were rated highly effective, implemented and low cost to implement
- Six remaining Outages:

- 1- Under-engineered for load
- 1- Lightning
- 4- Engine/hardware failure
- 3- Multiple failures
- 1- Remote location in the mountains, bad weather forced back helicopter and SnowCat trip was over 4 hours.

Procedural (PR)

The Team identified all procedural Best Practices from the original Switching, Signaling and DCS Focus Areas. A number of them were duplications of the same concepts or procedures within each of the 3 Focus Areas. These were rewritten to make them more generic across all Focus Areas as well as any new technologies. The Team also reviewed the Final Report of the NRSC Procedural Errors Team and identified 7 additional Best Practices from that report (PR27-PR33).

After reviewing the procedural outage reports . The Best Practice Team concluded that the volume of procedures being performed in the networks is increasing (increased opportunity for errors) due to the:

- Increasing complexity and capacity of operating environment
- Increased number of interconnecting networks
- Expanded capabilities of new technology
- Code openings due to increased utilization of numbering resources
- Implementation of Number Portability
- Y2K related software changes

The Best Practice by Best Practice review of survey responses indicated that the Procedural Best Practices have:

- High Implementation
- However, Implementation may mean “have a policy”
- Are highly effective however, in practice, the trend in the frequency of procedural outage reports indicate that they are not being followed
- Are directed at both mitigating and preventing outages

Essential Services

The report of the Essential Services Committee of NRC II contained 33 recommendations which posed many options and alternatives to improve reliability. These were mapped directly into 33 Best Practices by the first Best Practice Team. The current Best Practices Team determined many of the 33 recommendations were complementary and supplementary or alternatives to each other. Survey Data indicated confusion regarding implementation responses. As a result the Best Practice Team completely revamped the 33 Essential Services Best Practices which:

- Deleted redundant BPs
- Deleted “Not Best” Practices
- Combined related options and alternatives that supported the same goals and objectives into single Best Practices.

As an example, ES01- Called for diverse Interoffice Transport Facilities, ES02 - Diverse Interoffice Transport Facilities with Standby Protection (Option of ES01) offered one method of providing diversity, ES03 - Diverse Interoffice Transport Facilities Using DCS (Option of ES01) provided an alternative method. ES04 - Fiber Ring Topologies for 911 Circuits accomplishes the goals of ES01,02&03 combined.

The original 33 Best Practices were mapped to 18 new Best Practices as follows:

- 33 Best Practices Evaluated
- 8 Deleted
- 7 combined with others

Facilities (FC)

The new set of Best Practices includes the latest Best Practices as defined by the NRSC Facility Solutions Team (FST). The Best Practice Team agreed that the FST had the industry expertise to address the Facility Best Practices and that it had been reviewing them since it was formed after NRC I.

Fire (FR)

The Original Fire Best Practices from NRC II & I were imported in their entirety. While fire related outages have not been a significant contributor to network unreliability, the original Best Practices are still appropriate.

Network Elements (NE)

These Best Practices were not part of the survey as they were not related to Power, Facilities, Essential Service, or Procedural. They were originally in the Signaling or DCS Focus areas and have been expanded and made more generic to make them applicable to all network elements.

Supplier (SP)

The Supplier Best Practices were expanded to read more like Best Practices and were updated to make them more relevant to the current supplier environment. The other observations are:

- SP05 Human factors represents a new paradigm for vendors. There will be increased "emphasis" due to the Procedural Errors Team Report.
- SP12 Establish Core Team to plan, test and evaluate change - Service Provider initiated BP that suppliers should participate in. Not a Supplier BP Delete (See PR14)
- Add PR04 Information Sharing Guidelines - as SP12
- Survey reflects continued high implementation
- Confirmed broad industry applicability beyond traditional Telcom suppliers
- Combined categories of DCS, Switch and Signaling into 1 Network element category

Recommendations

Service Providers

The Best Practice Team reviewed the complete list of Best Practices, for application to the service provider segment of the Telecommunications Industry and recommends full implementation of the following Best Practices:

POWER (PW) Best Practices

PW01 Place strong emphasis on human activities related to the operation of central office power systems (e.g. maintenance procedures, alarm system operation and response procedures, and training for craft personnel).

PW02 Provide diversity so that single point failures are not catastrophic.

PW03 Adhere to telecommunications industry existing power engineering design standards.

PW04 Service Providers should retain complete authority about when to transfer from the electric utility and operate standby generators.

PW05 Service Providers should not normally enter into power curtailment or load sharing contracts with electric utilities.

PW06 Service Providers and electric utilities should plan jointly to coordinate hurricane and other disaster restoration work.

PW07 Dual commercial power feeds with diverse routing from separate substations should be provided for the most critical network facilities and data centers.

PW08 Service Providers should establish a general requirement for some level of power conditioning or protection for computers and sensitive electronic equipment.

PW09 Design standby generator systems for fully automatic operation and for ease of manual operation, when required.

PW10 Maintain adequate fuel on-site and have a well-defined re-supply plan. HIGHLY RECOMMENDED

PW11 Provide automatic reserve lubricating oil makeup systems for extended operation of diesels.

PW12 Have a well-defined plan that is periodically verified for providing portable generators to offices with and without stationary engines in the event of an engine failure.

PW13 Service Providers should routinely exercise engines with load.

PW14 Service Providers should run engines for an extended period, at least 5 hours, with all available loads annually.

PW15 Coordinate engine runs with all building occupants to avoid interruptions.

PW16 For large battery plants in critical offices provide dual AC feeds (odd/even power service cabinets for rectifiers).

PW17 The two transfer breakers (in power transfer systems) must be mechanically and electrically interlocked.

PW18 Transfer switches (UL standard 1008) should be used in lieu of paired breakers.

PW19 Provide indicating type control fuses on the front of the switchboard.

PW20 Provide color- coded mimic buses showing power sources, transfer arrangements, essential/nonessential buses, etc.

PW21 Post at the equipment (or have readily available) single line and control schematics.

PW22 Keep circuit breaker racking/ratchet tools, spare fuses, fuse pullers, etc. on hand.

PW23 Clearly label the equipment served by each circuit breaker.

PW24 Provide emergency procedures for AC transfer.

PW25 Train local forces on AC switchgear to understand procedures and stage occasional rehearsals.

PW26 Provide surge arrestors (TR-NWT-001011) at the AC service entrance of all Service Provider equipment buildings.

PW27 Design a professionally administered preventive maintenance program for each company's electrical systems.

PW28 Provide a minimum of 3 hours battery reserve for central offices equipped with fully automatic standby systems.

PW29 All new power equipment, including batteries should conform to NEBs.

PW30 When valve regulated batteries are used, provide temperature compensation on the rectifiers.

PW31 A modernization program should be initiated or continued to ensure that outdated equipment is phased out of plant.

PW32 For new installations, multiple smaller battery plants should be used in place of single very large plants serving multiple switches, etc.

PW33 Low voltage disconnects should not be used at the battery plant. HIGHLY RECOMMENDED

PW34 The rectifier sequence controller should be used only where necessary to limit load on the engine.

PW35 Service Providers should consider and include the capabilities of smart controllers, monitoring, and alarm systems when updating their power equipment.

PW36 Manufacturers are encouraged to continue to improve the human-machine interfaces of power equipment.

PW37 Provide diverse feeds for SS7 links, BITS clocks, and other duplex circuitry.

PW38 Provide protective covers and warning signs on all vulnerable circuit breakers.

PW39 Ensure that the fuses and breakers meet quality level III reliability.

PW40 Power wire, cable, and signaling cables that meet NEBS should be required in all telecommunications locations.

PW41 Wherever possible, DC power cables, AC power cables and telecommunications cables cable should not be mixed.

PW42 Verify DC fusing levels, especially at the main primary distribution board to avoid over fusing.

PW43 Detailed methods and procedures are needed to identify all protection required around the energized DC bus. HIGHLY RECOMMENDED

PW44 Update installation handbook to include verification of front to rear stenciling.

PW45 Perform high-risk operations during low traffic periods.

PW46 Procedures and restoral processes are required for any cable-mining job. HIGHLY RECOMMENDED

PW47 Each company must have an alarm strategy.

PW48 Provide a separate "battery discharge" alarm for all battery plants. Program the alarm to repeat (e.g,.at least every 15 minutes). HIGHLY RECOMMENDED

PW49 Redundancy must be provided, so that no single point alarm system failure will lead to a battery plant outage.

PW50 Highlight the battery discharge (and other critical alarms) at the remote center.

PW51 For critical alarms produced by single contacts (one on one), use "normally closed" contacts that open for an alarm.

PW52 Power monitors should be integrated into engineering and operational strategies.

PW53 Maintain the power alarms by testing the alarms on a scheduled basis.

PW54 Provide hands-on training for operation and maintenance of power equipment.

PW55 Place utmost emphasis on the maintenance and response to power alarms.

PW56 Emphasize: use of methods of procedures (MOPs); vendor monitoring; and performing work on in-service equipment during low traffic periods. HIGHLY RECOMMENDED

PW57 On removal projects, check for current flow in power cables with AC/DC clamp-on ammeters.

PW58 Provide and test detailed action plans to address emergency situations, such as when both the commercial AC power and the standby engine fails to start.

PW59 Perform annual evaluation/maintenance of all power equipment.

PW60 Use infrared thermographic scanners to check power connections.

PW61 Employ the "Ask Yourself" program to supplement conventional training.

PW62 Vendors should provide clear and specific engineering, ordering, and installation in support of their products.

PW63 Service Provider personnel should evaluate support documentation as an integral part of the equipment selection process.

PW64 Operating personnel must be familiar with support documentation provided with the equipment.

PW65 Service Providers should have documented installation guidelines that apply in their company. HIGHLY RECOMMENDED

PW66 Service Providers should clearly communicate their installation guidelines to all involved parties. HIGHLY RECOMMENDED

PW67 On-site installation acceptance should include a quality review of conformance to the company's and vendors installation guidelines. HIGHLY RECOMMENDED

PW68 Service Providers should have procedures for pre-qualification or certification of installation vendors.

PW69 In preparation for a hurricane, place standby generators on line and verify proper operation of all subsystems. LIMITED APPLICATION

PW70 In coastal areas, design standby systems to withstand high winds, wind-driven rain and debris. LIMITED APPLICATION

PW71 Improve fuel systems reliability. Provide redundant pumps for day tanks and a manual-priming pump.

PW72 Reemphasize the need for local procedures and contingency plans for power emergencies.

PW73 Reemphasize the need for power expertise/power teams.

PW74 Provide security from theft of portable generators. Trailer mounted generators equipped with wheel locks are recommended.

ESSENTIAL SERVICES (ES) Best Practices

ES01 Diverse Interoffice Transport Facilities - When all 9-1-1 circuits are carried over a common interoffice facility route, the Public Safety Answering Point (PSAP) has increased exposure to possible service interruptions related to a single point of failure (e.g., cable cut). The 9-1-1 circuits should be placed over multiple, diverse interoffice facilities.

Diversification may be attained by placing half of the essential communication circuits on one facility route, and the other half over another geographically diverse facility route (i.e., separate facility routes). Many LECs deploy diverse interoffice facility strategies when diverse facilities are already available.

Option 1: Diverse Interoffice Transport Facilities with Standby Protection - A variation of the facility diversity architecture is deployment of a 1-by-1 facility transport system. This architecture is protected by a standby protection facility that is geographically diverse from the primary facility. Because no calls are lost while switching to the alternate transport facility during primary route failure, this architecture is considered self-healing.

Option 2: Diverse Interoffice Transport Facilities Using DCS - Earlier NRC Focus Group recommendations suggested using diverse interoffice transport facilities from the called serving end office via two diverse Digital Cross-connect Systems (DCS) for concentration. This approach provides diversity and, due to the concentration by the DCS network elements, offers a less costly network solution.

Option 3: Fiber Ring Topologies for 9-1-1 Circuits - Fiber optic network elements offer network service providers the ability to aggregate large amounts of call traffic onto one transport facility. Traffic aggregation opposes the diverse facility transport recommendations defined in this document. However, fiber rings permit a collection of nodes to form a closed loop whereby each node is connected to two adjacent nodes via a duplex communications facility. Fiber rings provide redundancy such that services may be automatically restored (self-healing), allowing failure or degradation in a segment of the network without affecting service. Fiber rings are used in some metropolitan areas, ensuring essential communications service is unaffected by cuts to fibers riding on the ring. Ring features and functionality are part of the Synchronous Optical Network (SONET) technical requirements. When essential communications is placed on SONET rings, service interruptions are minimized due to the self-healing architecture employed.

ES02 Red-Tagged Diverse Equipment - Depending on LEC provisioning practices, the equipment in the central office can represent single points of failure. 9-1-1 circuits should be spread over similar pieces of equipment, and marking each plug-in-level component and frame termination with red tags. The red tags alert LEC maintenance personnel that the equipment is used for critical, essential services and is to be treated with a high level of care.

ES03 **Option 1:** Alternate PSAPs from the 9-1-1 Tandem Switch - A common method of handling PSAP-to-Tandem transport facility interruptions is to program the 9-1-1 tandem switch for alternate route selection. If the 9-1-1 caller is unable to complete the call to the PSAP, the tandem switch would automatically complete the call to a pre-programmed directory number or alternate PSAP destination. The alternate

PSAP may be either administrative telephones or another jurisdiction's PSAP positions, depending upon the primary PSAPs pre-arranged needs.

Option 2: Alternate PSAPs from the Serving End Office - Another method of handling PSAP-to-Tandem transport facility interruptions is to program the end office for alternate route selection. If the 9-1-1 caller is unable to complete the call to the PSAP, the end office switch may automatically complete the call to a pre-programmed directory number or alternate PSAP destination. The alternate PSAP may be either administrative telephones or another jurisdiction's PSAP positions, depending upon the primary PSAPs pre-arranged needs.

ES04 **Option 1:** PSTN as a Backup for 9-1-1 Dedicated Trunks - To ensure that 9-1-1 is minimally affected by potential traffic congestion sometimes experienced in the Public Switched Telephone Network (PSTN), PSAPs commonly create dedicated private public safety networks.

A low-cost alternative for handling 9-1-1 calls during periods of failure in the end office-to-9-1-1 tandem transport facility, is to use the PSTN as a backup between the caller's end office and the 9-1-1 tandem switch. Such applications may or may not make use of adjunct devices that monitor primary trunk path integrity.

If the primary path to the 9-1-1 tandem switch should be interrupted or all-trunks-busy, the call may be forwarded over the PSTN to a preprogrammed directory number. Further, the caller may be identified if the administrative line is equipped with a caller identification (ID) device.

Option 2: Wireless Network as Backup for 9-1-1 Dedicated Trunks - Similar to the PSTN backup for completing 9-1-1 calls when the primary transport facility is interrupted, wireless networks may provide more diversity than the PSTN alternative. (See Figure 6-7) As in Best Practice ES08, an adjunct device may or may not be used to monitor the primary trunk path integrity.

ES05 Intraoffice 9-1-1 Termination to Mobile PSAP - Commonly, the transport facility between the PSAP and the serving end office may not have facility route diversity. To accommodate instances where these facilities are interrupted or it becomes necessary to evacuate the PSAP location, some PSAPs have established mobile PSAP systems that may be connected to phone jacks at the serving end office. The phone jacks, although usually installed inside the end office for security purposes, are typically installed in an accessible location for ease in locating them during an emergency.

Some PSAPs have prearranged with the serving LEC to permit a jurisdictional employee having an emergency vehicle (e.g., police car) equipped with radio capability to retain a key to the LECs end office and to connect to an RJ-11 jack for 9-1-1 call interception. Another type of receptacle may be pre-installed in the end office for connection to a mobile PSAP.

ES06 Dual Active 9-1-1 Tandem Switches - Dual active 9-1-1 tandem switch architectures enable circuits from the callers serving end office to be split between two tandem switches. Diverse interoffice transport facilities further enhance the reliability of the dual tandem arrangement. Diversity is also deployed on interoffice transport facilities connecting each 9-1-1 tandem to the PSAP serving end office.

ES07 TOPS as a 9-1-1 Tandem Backup - Operator services tandem switches can also serve as backup and/or overflow for network elements, due to their ubiquitous connectivity throughout the telephone network. In most instances, existing trunking and translations may be used when adding a Traffic Operator Position System (TOPS) to the 9-1-1 network.

When an interoffice transport facility fails or an all-trunks-busy condition occurs, the backup/overflow route to the operator services tandem is selected. The operator tandem switch recognizes the call as an emergency by translating the 9-1-1 dialed digits, and may be preprogrammed to automatically route the call to the serving 9-1-1 tandem switch.

Further, if the operator tandem switch is unable to access the 9-1-1 tandem switch, the call will automatically be "looped around" so that an operator may manually answer the call and manually attempt to reach emergency services providers.

ES08 Local Loop Diversity - The local loop access is defined as that portion of the network which connects the caller (i.e., the subscriber or the PSAP) to the network serving end office. The local loop is potentially a single point of failure.

Although it is unlikely the subscriber will purchase diverse transport facilities for typical PSTN service, PSAP local loops should be diverse where possible and/or make use of wireless technologies as a backup for local loop facility failure (e.g., cable cuts).

ES09 Network Management Center and Repair Priority - Network management centers (NMCs) should remotely monitor and manage the 9-1-1 network components. The NMCs should use network controls where technically feasible to quickly restore 9-1-1 service and provide priority repair during network failure events.

ES10 Diverse Automatic Location Identification (ALI) Data Base Systems - ALI systems should be deployed in a redundant, geographically diverse fashion (i.e., two identical ALI data base systems with mirrored data located in geographically diverse locations).

Deployment of fully redundant ALI data base systems, such that ALI system hardware and/or software failure does not impair ALI data accessibility, will further improve ALI reliability. When deployed with geographically diverse transport facilities, single points of failure may be eliminated.

The NRC also recommends placement of the ALI data on fault-tolerant computer platforms to increase the reliability of ALI display retrievals. Finally, "hot spare" computers should be held in reserve for catastrophic events.

ES11 Move Mass Calling Stimulator away from 9-1-1 Tandem Switch - Mass calling events may cause 9-1-1 service interruptions. Service interruptions caused by media stimulated calling has prompted the LECs to reassess and improve the handling of mass calling events. The 9-1-1 Tandem switch serves as the most critical network element in providing 9-1-1 service. If a media stimulated mass calling event is served by the 9-1-1 Tandem, the PSAPs being served by the 9-1-1 Tandem may experience delayed dial tone when call transfer is attempted by the PSAP personnel. The PSAP may also experience delays in call completion (ring-back tone) or a fast busy signal, which indicates that the call has failed to complete. To mitigate such instances, high volume call events should be moved to another end office.

Pre-Planning for Mass Calling Events - To minimize the potential of interruption caused by media driven mass calling events, the LEC can identify periods of low call volume traffic so that the media may schedule mass calling events during low traffic periods.

Carrier external affairs and marketing groups should work closely with media organizations to ensure 9-1-1 callers are unaffected by mass calling events.

ES12 Contingency Plan Training - Once a contingency plan is developed, it should be periodically tested. These tests can be of various types:

- Desktop check tests (using a checklist to verify familiarity of "what to do in case of").
- Procedures verification test (verify that established procedures are followed in a simulation).
- Simulation test (similar to a fire drill, e.g., simulating a disaster and monitoring the response).
- Actual operations test (cause an event to happen, e.g., power or computer failure and monitor the response).

The importance of testing a contingency plan is critical to its success. An annual schedule of testing and evaluating written results is an excellent method of ensuring that a plan will work in the event of a disaster and for identifying weaknesses in the plan.

Close cooperation between a service provider and the PSAP in conducting actual operations testing will be of mutual benefit to both the service provider and the PSAP. An annual comprehensive operational test of the contingency plan is strongly encouraged.

ES13 Educate the Public on Proper Use of Essential Communications - The public's proper use of 9-1-1 service is critical to the effectiveness of the emergency network's operation. Misuse of 9-1-1 could lead to the following:

- Congestion of the 9-1-1 network, leaving callers with real emergencies unable to contact a 9-1-1 operator.
- Exhaustion of resources on non-emergency situations.

- Reduction in a jurisdiction's ability to respond to emergency situations in a timely manner because of the jurisdiction's emergency response agencies being overwhelmed by responses to non-emergency situations.

This could have potentially disastrous effects on the public's perception of its emergency network and emergency response agencies.

ES14 Improve Communications among Network Providers and PSAPs - Network service providers, 9-1-1 administrators, and public safety agencies should continually strive to improve communications among themselves. They should routinely team to develop, review, and update disaster recovery plans for 9-1-1 disruption contingencies, share information about network and system reliability, and determine user preferences for call overflow routing conditions.

They should actively participate in industry forums and associations focused on improving the reliability of emergency services and the development of technical industry standards. The National Emergency Number Association (NENA) and the Association of Public-safety Communications Officials (APCO) are just two of the organizations that are open to all stakeholders of 9-1-1 service delivery and that are focused on finding 9-1-1 solutions for emerging technologies (e.g., wireless, PBX, CLEC).

ES15 Critical Response Link Redundancy/Diversity - The redundancy and diversity concepts set forth in ES01 should be applied to other network links considered vital to a community's ability to respond to emergencies. Types of links that are critical to the provision of emergency aid include communication links from the PSAP location to:

- Law enforcement dispatchers and/or response personnel.
- Emergency medical service (EMS) dispatchers and ambulance response units.
- Fire fighter dispatchers and response personnel.
- Poison control centers and other agencies offering remote diagnostic information and advice on how to respond to requests for emergency aid.
- Trauma centers and similar emergency hospices.

Standards must be established to address interconnection issues between PSAP and CMRS/cable television service providers.

Media and Repair Link Redundancy/Diversity - the redundancy and diversity concepts set forth in ES01 also should be applied to network links considered vital to a community's ability to respond to emergencies. Types of links that are critical to the provision of emergency aid during such events include communication links from the PSAP location to broadcast media organizations and local network provider repair centers.

Media organizations can alert the public during periods of emergency network degradation or outage through appropriately worded public service announcements, relieving excessive call volumes, and making the public aware of interim emergency aid access alternatives.

In addition, dedicated network links and/or alternate accesses to network provider repair personnel will ensure that interruptions are known immediately and that repair personnel are mobilized expeditiously.

ES16 Private Switch (PS)/Alternative LEC (CLEC) ALI - ALI data for alternate providers (PS, CLEC, etc.) should be included in the ALI systems. The FCC should pursue closure on those issues remaining for Docket 94-102, and to require affected service providers to participate in PSAP PSALI programs.

PSAPs have become increasingly reliant on the ALI data administered by the LECs, and believe that those individuals served by private telecommunication providers and/or alternate LEC providers should have their address information contained in their ALI data base systems. The NENA Recommended Formats for Data Exchange and the NENA Recommended Protocols for Data Exchange were established to enable ALI data integration of these providers.

ES17 CMRS - Emergency Calling - The CMRS industry should consider 9-1-1 as the standard access code for emergency services, such as law enforcement, fire, EMS. Implementation of such a standard would eliminate confusion among mobile communications users when they are in a roaming mode. **See FCC Docket 94-102, WT Report Number 99-32 (released November 18, 1999), FCC Docket 94-102 RM 8143, and FCC 99-245.**

ES18 Outage Reporting - All providers of essential communications **should** have a uniform method of reporting and tracking significant service outages for internal use and, where required, for outage reporting to the FCC. Root cause analysis, publication of results and new best practices may be left up to the industry.

PROCEDURAL (PR) Best Practices

PR01 Awareness Training - There is a critical need for a broad based educational system for all field and management personnel involved in the operation, maintenance, and support of Network Elements. The Awareness Training must stress the importance of end to end communications for all persons involved in maintenance activities on these systems. A successful program must educate its target audience on the technology, its benefits and risks, and the magnitude of traffic carried. The training must emphasize the functionality and the network impact of failure of active and standby (protect) equipment in processors, interfaces, peripheral power supplies, and other related components, and the identification of active and standby (protect) units. Special emphasis should focus on the systematic processes for trouble isolation and repair.

PR02 Technical Training - Service providers should establish a minimum set of work experience and training courses which must be completed before personnel may be assigned to perform maintenance activities on network elements, especially when new technology is introduced in the network.. This training must stress a positive reinforcement of procedures at all times. The use of signs designating various work areas, labels on equipment and cabling, properly identified inventory storage areas, log sheets for work performed, and procedures to be followed in case of emergencies. This training must also emphasize the steps required to successfully detect problems and to isolate the problem systematically and quickly without causing further system degradation. Special emphasis should be placed on maintaining and troubleshooting problems related to system power equipment which can add significant delay to restoration activities.

PR03 MOPs and Acceptance/Verification Check-Off Sheets for Hardware and Software Growth/Change Activities - Methods of procedure (MOPs) should be prepared for all hardware and software growth and change activities. As far as practicable, the MOP should be prepared by the people who will perform the work. The MOP should be approved by the responsible engineer, line operations manager, installation manager, and others, as appropriate; and deviations from the documented process should also be approved by this team. When it is necessary to reference other documents in the MOP, these references should be detailed and include appropriate issue/date information. The MOP should identify each step required to perform the work. As each work function is completed, it should be signed off in the MOP. An acceptance/verification testing che ck-off sheet should also be utilized to assure that the work activity was performed correctly. . HIGHLY RECOMMENDED

PR04 Information Sharing Guidelines - Industry Guidelines for the Sharing of Information about network outages is included in the NIIF Reference document Part VII. This document is intended to provide the appropriate guidance to facilitate the sharing of information. It identifies types of information which may be shared, the circumstances under which it should be shared, the extent to which sharing is appropriate, and the mechanisms and timing for that sharing. It represents industry consensus arrived at with the full participation of members of the Network Interconnection Interoperability Forum which consists of Access Service Providers, Access Service Customers and Vendor/Manufacturers.

PR05 Centralized Control for Network Elements - It is recommended that service providers provide centralized maintenance, administration, surveillance and support for all network elements. Monitoring and control should be in as few places as possible to provide consistency of operations and overall management.

PR06 Training in Trouble Detection and Isolation - Lack of troubleshooting experience and proper training in this area usually prolongs the trouble detection and isolation process. It is recommended that network operators be adequately trained in the trouble detection and isolation process.

PR07 Outage Information Sharing - A prime source for information concerning outages is the network outages reported to the FCC as required by Section 63.100 of the rules. Final reports of all 1999 outages are posted at www.fcc.gov/Bureaus/Engineering_Technology/Filings/Network_Outage/1999/report.html. The final reports for 1996, 1997, and 1998 are also available simply by changing the year in the above URL. The posted reports are Adobe Acrobat pdf (portable document format) scans of the reports provided by the carriers. Review of the reports will enable the reader to become aware of significant problems impacting the network.

PR08 Maintaining Link Diversity - Industry Guidelines for Maintaining Link Diversity can be found in the NIIF Reference Document, Part III, Attachment G. The following are some of the Operating Principles of the document: Link diversification validation should be performed at a minimum of twice a year, at least one of those validations shall include a physical validation of equipment compared to the recorded documentation of diversity.

- The validation of diversification is the responsibility of every network service provider that provides or utilizes SS7 links.
- Limitations on diversification should be considered at the time of deployment, such limitations may consist of, geography, facilities, circuit design and tariffs.

PR09 off-peak Scheduling (Formerly SN-03) - High risk, potentially service affecting maintenance and growth procedures should be scheduled during weekend and off-hours.

PR10 Review Rehome Procedures - Network service providers carefully review all rehome procedures and undertake meticulous pre-planning before execution. Communication to all inter-connected networks will be essential for success in the future. It is also important to make sure that rehome procedures are carefully followed.

PR11 Review Detection & Manual Intervention Procedures - Network operators should be adequately trained in (1) detection of conditions requiring intervention, (2) escalation procedures, and (3) manual recovery techniques.

PR12 Develop Crisis Management Exercises - During the past several years a number of disastrous events, the Oklahoma City bombing, the Midwest flooding, earthquakes in California and hurricanes in Louisiana, Florida and Hawaii, have prompted an increased awareness on the part of all members of the telecommunication industry to the critical need to have a Disaster Preparedness strategy. This strategy should outline a network service provider's Disaster Preparedness organization, the roles, responsibilities and training of its members and provide for cooperative interaction among both internal and external organizations. The purpose of this strategy is to provide for the development of emergency plans that protect employees, ensure service continuity and provide for the orderly restoration of critical services in the event of a major network catastrophe.

PR13 Test a Network's Operational Readiness through planned drills or simulated exercises. Service Providers should conduct exercises periodically keeping the following goals in mind:

- The exercise should be as authentic as practical. Scripts should be prepared in advance and team members should play their roles as realistically as possible.
- While the staff must be well prepared, the actual exercise should be conducted unannounced in order to test the responsiveness of the team members and effectiveness of the emergency processes. Also, callout rosters and emergency phone lists should be verified.
- Early in the exercise, make sure everyone understands that this is a disaster simulation, not the real thing! This will avoid unnecessary confusion and misunderstandings that could adversely affect service.
- It is particularly important to coordinate disaster exercises with other Service Providers and vendors.
- It is very important immediately following the drill to critique the entire procedure and identify "lessons learned". These should be documented and shared with the entire team.

PR14 Validate Upgrades, new procedures and commands in Lab. All Service Providers should establish and document a process to plan, test, evaluate and implement all major change activities onto their network. This industry best practice describes a process that should include:

- The establishment of a multi-discipline core team, which includes suppliers, to plan and implement changes. The team's focus should be on planning, testing, and evaluation of all major network elements and systems.
- The validation of all upgrades and procedures in a lab environment prior to the first application in the field.
- The creation of a "Methods of Procedure (MOP)" for each change activity that outlines the maintenance steps to be taken and an emergency restoration plan.

Finally, it is highly recommended that, in response to the ever-increasing amount of change activity being performed, each Service Provider establish a "Change Management Control" (CMC) group to act as a customer advocate.

PR15 Restrict Commands Available to Technicians to Ensure Authorized Access and Use.

PR16 Establish Procedure to Reactivate Alarms After Provisioning - The volume of alarms during provisioning create a potential for alarm saturation and makes it very difficult to differentiate between a real alarm and those caused by other activities. A common practice is to simple inhibit these alarms or set their thresholds so high they do not report. The danger here is that there must be a fail-safe measure to turn these alarms back on when the facility is carrying traffic.

PR17 Schedule System Backups - All Service Providers should establish policies and procedures that outline how critical network element databases, (e.g. digital cross connect system databases, switching system images), will be backed up onto a storage medium (tape, optical diskettes, etc.) on a scheduled basis. These policies and procedures should address, at a minimum, the following:

- Database backup schedule and verification procedures
- Storage medium standards
- Storage medium labeling
- On site and off site storage
- Maintenance and certification
- Handling and disposal

The implementation of this practice will mitigate the impact of data corruption or some other loss of a critical network database.

PR18 Companies should appoint a Synchronization Coordinator for their company who will perform the responsibilities contained in SR-2275. Companies should provide the name of their Synchronization Coordinator to the NIIF for inclusion in its Company Specific Contact Directory.

PR19 Companies should comply with the synchronization standards addressed in the ANSI Standard T1.101, entitled "Digital Network Synchronization"

PR20 Bilateral agreements should be established between interconnecting network providers, referencing the NIIF Interconnection Template document.

PR21 Bilateral agreements between interconnecting networks should address the issue of fault isolation. At a minimum, these agreements should address the escalation procedures to be used when a problem occurs in one network. Second, the agreement should address which company will be in charge for initiating various diagnostic procedures. Finally, the agreement should address what information will be shared between the interconnected companies.

PR22 To keep overflow traffic conditions from adversely affecting interconnected networks, interconnected network providers should utilize network surveillance and monitoring. In addition, companies should follow the guidelines for advanced notification of media-stimulated call-in events as outlined in Part 6 of the NIIF Reference Document concerning Media Stimulated Call-in Events. Further, interconnecting companies should include a contact name for inclusion in the Company Specific Contact Directory. Finally, interconnecting companies should address the control of overflow conditions in their bilateral agreements.

PR23 Information sharing should be utilized by all network providers to minimize recurrence of service disruptions. The guidelines contained in the NIIF Reference Document can be used for this purpose. Additional requirements for the sharing of information between interconnected companies should be addressed in bilateral agreements.

PR24 New entrants should, at a minimum, have a communications structure in place for timely notification of affected parties in the event of disasters or emergencies.

PR25 Companies should appoint and provide the name of a Mutual Aid Coordinator to the NIIF for inclusion in the Company Specific Contact Directory which is published on a bi-annual basis.

PR26 Telecom service suppliers and vendors should adopt the concept of a simplified language system, which controls vocabulary, grammar, mechanics, and style for better user understanding.

PR27 Telecommunication equipment suppliers should adopt uniform methods of electronic documentation distribution and usage. Electronic access to documentation will allow better version control and ease of access for field personnel. Additionally, electronic access allows implementation and delivery of future enhancements such as interactive methods and information.

PR28 A physical verification of both local and remote alarms and of remote network element maintenance access should be performed on all new equipment installed in the network before it is placed into service. When these functions are not performed, the probability of failure without notification is greatly increased. Likewise, if remote network element access is not verified, a simple restoration process may require technician dispatch to the site, resulting in further delay in service restoral.

PR29 If a new CO is installed or an old switching system replaced, the integrity of the diversified FX telephone line for the office should also be verified.

PR30 A number of outages are of extended duration because the technician does not have the tools nor test equipment to implement the restoration. The most common cause is unavailability of spare circuit packs. This results in a delay until the spares are located and shipped from some other location. To prevent these delays, a process should be established to track the location of all spare equipment. This process should align with network performance and reliability requirements and should include procedures for allocating, procuring, delivering, and deploying spare equipment. When spares are not locally available, the process should also provide a method to expedite identification and delivery of the required equipment.

PR31 All removable covers that have equipment designations should have those designations removed and the designations placed on the permanent portion of the unit or frame.

PR32 The most effective practice when performing complex translation changes is to test the translations before and after the change to ensure the appropriate and expected results.

FACILITY (FC) Best Practices

FC01 Adhere to formal damage prevention and restoration procedures.

FC02 Use Warning Tape - place tape 12 in. above the cable system.

FC03 Visible Cable Markings (unless prone to vandalism).

FC04 Timely response to all locate requests.

FC05 Enhanced Locating Equipment - use current, and/or emerging technologies; upgrade locating equipment as new technologies emerge.

FC06 Use of Plant Route Maps - secondary checking of plant drawings relative to marking.

FC07 Dig Carefully - When excavation is to take place within the specified tolerance zone, the excavator exercises such reasonable care as may be necessary for the protection of any underground facility in or near the excavation area. Methods to consider, based on certain climate and geographical conditions include: hand-digging when practical (potholing), soft digging, vacuum excavation methods, pneumatic hand tools, other mechanical methods with the approval of the facility owner/operator, or other technical methods that may be developed.

FC08 Assign trained technical personnel to monitor activities at work sites where digging is underway.

FC09 Cooperation With Contractors - easy access, open communications with contractors.

FC10 Training - continuous refresher training.

FC11 Contractor Awareness - public service seminars, literature and announcements.

FC12 Contact With Land Owners - proactively educate and communicate with right-of-way owners.

FC13 Develop employee program to recognize, report and prevent potential cable damage.

FC14 Audits/Surveys of Plant - periodically check and validate and update outside plant records and data.

FC15 Limited placement of barriers around above ground structures to prevent damage.

FC16 Buried Cable - bury fiber cable in accordance with standards and plans.

FC17 Buried Facilities - bury structures out of sight and to appropriate depths.

FC18 Protective Devices - use rodent devices on poles and cable sheaths in rodent infested areas.

FC19 Stronger Conduit - use type B pipe in rodent infested areas.

FC20 Secure access points such as manholes, cabinet vaults, etc.

FC21 Improve the effectiveness of state one-call legislation.

FC22 Increase stakeholder coordination and cooperation on state one-call legislation efforts.

FC23 Establish a dedicated Cable Damage Awareness/Prevention Program with excavators, locators, and municipalities.

FC24 Identify critical routes and provide these routes with additional protection.

FC25 Promote the development of industry standard markings.

FC26 Establish training, qualification and performance standards of internal and external utility locators.

FC27 Design and place new facilities to minimize risk (for example, underground, in conduit, in interduct, etc.).

FC28 Provide physical diversity on critical routes when justified by a thorough risk/value analysis.

FC29 Take active role on One-Call Board and solicit information from other stakeholders.

FC30 Jointly relocate facilities.

FC31 Employ courtesy or mutual right of way jeopardy notification.

FC32 Evaluate the performance of contracted excavators and internal excavators.

FC33 Develop and implement a rapid restoration program.

FC34 Assess and implement most of the DCS Focus Group's Recommendations when operating large SONET/ATM Add Drop Multiplexer (ADM).

FC35 Take additional precautions when the newest technologies (untried).

FC36 Track and analyze facility outages. Take action if any substantial negative trend arises or persists.

FC37 Follow the excavator best practices described in the Minimum Suggested Damage Prevention Guidelines - Excavation Procedures for Underground Facilities.

FC38 Conform to the Minimum Performance Guidelines for One-Call Notification Systems.

FC39 Conform to the Minimum Guidelines for Facility Owners.

FC40 Conform to the Guidelines for Prospective Excavation Site Delineation and Location Markout. This includes white lining.

FC41 Ensure that federal one-call legislation is used to bring all states up to high level of damage prevention.

FIRE (FR) Best Practices

FR01 Develop Pre-plans with Fire Agencies

FR02 Verify Smoke/Heat Detection Capability

FR03 Meet NEBS Requirements for Power & Communication Cables

FR04 Consider Non-reuse of Noncompliant Cable

FR05 Use ANSI T1.311-1998 "Standard for Telecommunications Environmental Protection, DC Power Systems" for COs

FR06 Test All Pre-1989 VRLA Batteries

FR07 Establish Case History File by Equipment Category for Rectifiers

FR08 Locate Transformers External to Buildings

FR09 Regularly Inspect Motors

FR10 Exercise & Calibrate Circuit Breakers

FR11 Use Defined Procedure for Cable Mining

FR12 Implement a Certification & Training Program for Contractors

FR13 Develop & Execute a Standard MOP for Vendor Work

FR14 Develop Site Management & Building Certification Program

FR15 Review Practices on Use of Soldering Irons

FR16 Prohibit Smoking in Buildings

FR17 Verify Aerial Powerlines are Not in Conflict with Hazards

FR18 Provide AC Surge Protection
FR19 Verify Grounding Arrangements
FR20 Assure Programs Exist for Alarm Testing
FR21 Avoid Use of Combustible Landscape Material
FR22 Verify Dumpster Location
FR23 Insure Proper Air Filtration
FR24 Administer Elevator Routines
FR25 Verify Elevator Building Compartments Comply with Code
FR26 Provide Smoke Detection and Ventilation in Motor Room
FR27 Use Over-current Protection Devices and Fusing
FR28 Inspect and Maintain HVAC areas
FR29 Restrict Use of Space Heaters
FR30 Establish Building Equipment Maintenance Program
FR31 Certified Inspection of Boilers & Fuel Storage Units
FR32 Provide All Critical Facilities with a Modern Smoke Detection System
FR33 Provide Automatic Notification of Local Fire Department
FR34 Implement Early Smoke Detection and Appropriate Ventilation Systems

NETWORK ELEMENT (NE) Best Practices (Non-Procedural)

NE01 Architectural and design alternatives – The following architectural and design alternatives should be evaluated:
-Two or more links per link set. With this design 3 or more simultaneous failures or errors must occur at the same time to cause a service interruption
-The use of dedicated DS1 facilities for links
-Use of quad A-links i.e., four diverse A-links to signaling points.

NE02 Placement of NEs in CO environment - In an effort to insure that maintenance procedures are consistent with other telephony network elements and the availability of qualified maintenance personnel are enhanced, network databases primarily used for call carrying / call handling functions (e.g. service control points (SCPs), network databases, etc) should be placed in a central office, telephony environment.

NE03 Carriers should improve their own failure data collection and analysis procedures for better root cause analysis. Carriers and suppliers should form partnerships to jointly perform this analysis.

NE04 Service Providers should develop and deploy a management system for use in circuit assignment, provisioning and maintenance, that will establish, monitor, track and maintain diversity of critical circuits

NE05 Provisioning: There must be a method to ensure synchronization of databases. An example is the transmission facility database and the DCS databases. These must be synchronized or an outage will occur. Procedures must also be in place to allow for manual provisioning in the event of a failure. It is also recommended that provisioning technicians be restricted from all commands except those that are needed for their work. Avoid any “global” commands that may have the potential for significant impact.

SUPPLIER (SUP)Best Practices

The Best Practice Team reviewed the complete list of Best Practices for application to the Supplier segment of the Telecommunications Industry and recommends full implementation of the following Best Practices:

SUP01 Software fault insertion testing (including simulating network faults such as massive link failures) should be performed as a standard part of a supplier's development process.

SUP02 Hardware fault insertion testing (including simulating network faults such as massive link failures) should be performed as a standard part of a supplier's development process. Hardware failures and data errors should be tested and/or simulated to stress SS7 fault recovery software.

SUP03 Fault recovery actions that result in significant loss of service need to be reviewed periodically by the manufacturers to assure that the least impacting strategies are being used for classes of failures implicated during root cause analyses.

SUP04 Initialization durations should be optimized to minimize service impact. Data from root cause analyses should be used to determine and improve specific areas of design.

SUP05 The manufacturers should place an added focus on human factors design to reduce human errors and/or reduce service-affecting impact of these errors.

SUP06 Carriers and suppliers should improve their own failure data collection and analysis procedures for better root cause analysis. Carries and suppliers should form partnerships to jointly perform this analysis.

SUP07 System suppliers should enhance existing, or establish new, standards for system robustness to prevent switching systems for accepting or allowing service affecting activity without a positive confirmation.

SUP08 System suppliers should provide a mechanism for feature adding/activation that allows for "Soft" activation rather than re-initialization. System supplier should provide an on-line memory management capability to reconfigure or expand memory without an impact on stable/transient call processing or the billing process.

SUP09 Hardware and software fault recovery design processes should converge early in the development cycle.

SUP10

Switching system suppliers should enhance their software development methodology to insure effectiveness and modern process of self-assessment and continual improvement. Formal design and code inspections should be performed as a part of the software development methodology.

A form of root cause analysis process is needed to investigate outage root causes and recommend corrective actions.
Test environments and scenarios should be enhanced to provide more realistic settings.
Fault tolerance requirements and standards need to be clarified.
Rigorous self-enforcement of design guidelines as they relate to system initializations.
Isolation of Faults/Containment of System Responses.
Continuous review of escalation strategy effectiveness based on field performance.

SUP11 A best practice from Sprint and NYNEX is to establish a multi-discipline Core Team, including the supplier; to plan, test, and evaluate all major change activities.

SUP12 All upgrades or growth procedures must be fully validated in the lab environment prior to first application in the field.

SUP13 Efforts should be made to eliminate the possibility of having a silent failure on any DCS system component, including the OS or Management System, cross-connect, or communications links.

SUP14 Service providers and equipment suppliers must work together to establish acceptable thresholds of equipment performance in the field environment.

SUP15 Documentation should be produced in a complete, easy-to-use, and timely manner, and is made accessible to the entire customer base. Customer input is essential! Documentation should be developed with a clear understanding of customer needs. The use of electronic media to maintain the documentation manuscripts and to access customer distribution information is essential.

SUP16 To keep tract of the numerous changes to both the product and the corresponding documentation, a change control database is recommended.

SUP17 The operations and maintenance manual should give an overview of the system and identify procedures for regularly scheduled operations. In addition, the documentation should be clear on how to manage unforeseen situations, including escalation to next level of technical support.

SUP18 An acceptance testing checkoff sheet should be developed and utilized during each new installation or addition.

SUP19 A comprehensive troubleshooting set of flowcharts (state diagrams) should be included in any set of documentation to guide all levels (both Tier 1-Novice and Tier 2-Expert) of maintenance support.

SUP20 As important as the human factor considerations are to the development of any telecommunications product, they are as equally important in the development of the documentation material

SUP21 Training should be developed with a clear understanding of customer needs. Customer input is essential! Once the training course is developed, it should again be thoroughly tested with the customer before being made generally available.

SUP22 Training must keep up with the numerous changes to both the product and its documentation material.

SUP23 Advance courses should be developed for personnel responsible for the technical support of various products, including operations supervisors, maintenance engineers, operational support personnel, and communications technicians. Training should not only cover local central office OAM&P needs, but also should cover all phases of remote centralized OAM&P.

SUP24

Establish and use metrics to identify key areas and focus, and measure progress in improving quality and reliability before and after general availability (this is described further as a recommendation in the following section).

Solicit and use customer feedback.

Perform detailed Root Cause Analysis for reported software faults and procedural errors. Based on these, use a total quality management approach to identify, plan, and implement improvements in the entire software process as well as processes associated with documentation & training.

SUP25 Critically review the level of inspection and surveillance on critical components. Do aggressive root cause analyses of field failures.

SUP26 Deploy systems on a going forward basis with redundant disk drives with common data or a new technology.

SUP27 Improved documentation on methods to recover from total as well as partial system outages.

SUP28 Where possible, and needed due to performance requirements, fully duplex, synchronized design should be implemented.

Acknowledgements

The Best Practice Team gratefully acknowledges the assistance and expertise provided by Norm Fischman and Charlie Romano of Bell Atlantic during our review of the Power Best Practices and outages.

The Best Practice Team also recognizes the leadership provided by Focus Group 3 Chairman, Ray Albers. Ray has kept us moving and on the straight and narrow. He was also a significant technical contributor to our work.

The Best Practice Team also appreciates the assistance provided by Judy Glatz, AT&T, in keeping our logistics straight and coordinating across the 2 sub-committees of Focus Group 3.

References

The Supplier Sub-committee references the following document used in the formation of the Supplier Best Practices.

Total Reliability Management for Telecommunications Software - Ming-Yee Lai and Karl F. Rauscher, IEEE Globecom '93: Communications for a Changing World, Houston, TX, pp. 505-509, 1993.

Appendices
A – Service Provider Questionnaire
B – Supplier Questionnaire
C – Facilities Questionnaire
D – Service Provider Questionnaire Results
E – Supplier Questionnaire Results
F – Facilities Questionnaire Results

	NRIC II Service Provider Best Practices Questionnaire				
	Please enter your company name:				
	Name of contact person: Phone No.:				
ID	**Recommendation**	*Purple* **Book Reference**	**Implementation (E-Everywhere, NE-Nearly Everywhere C-Critical Places Only, F-Few Places, N-Nowhere)**	**Effectiveness Rating (1- 5) (0-Don't Know)**	**Relative Cost to Implement (VL, L, M, H, VH)**
PW01	Place additional emphasis on human factors.	E-6.0			
PW02	Provide diversity so that single point failures are not catastrophic.	E-6.0			
PW03	Adhere to telecommunications industry existing power engineering design standards.	E-6.0			
PW04	Telcos should retain complete authority about when to transfer from the electric utility and operate standby generators.	E-6.19			
PW05	Telcos should not normally enter into power curtailment or load sharing contracts with electric utilities.	E-6.1.9			
PW06	Telcos and electric utilities should plan jointly to coordinate hurricane and other disaster restoration work.	E-6.1.9			
PW07	Dual commercial power feeds with diverse routing from separate substations should be provided for the most critical network facilities and data centers.	E-6.1.9			
PW08	Telcos should establish a general requirement for some level of power conditioning or protection for computers and sensitive electronic equipment.	E-6.1.9			
PW09	Design standby generator systems for fully automatic operation and for ease of manual operation, when required.	E-6.2.2			
PW10	Maintain adequate fuel on-site and have a well-defined re-supply plan.	E-6.2.2			
PW11	Provide automatic reserve lubricating oil makeup systems for extended operation of diesels.	E-6.2.2			
PW12	Have a well-defined plan that is periodically verified for providing portable generators to offices with and without stationary engines in the event of an engine failure.	E-6.2.2			
PW13	Telcos should routinely exercise engines with load.	E-6.2.2			

Appendix A Service Provider Best Practices Questionnaire

PW14	Telcos should run engines for an extended period, at least 5 hours, with all available loads annually.	E-6.2.2			
PW15	Coordinate engine runs with all building occupants to avoid interruptions.	E-6.2.2			
PW16	For large battery plants in critical offices provide dual AC feeds (odd/even power service cabinets for rectifiers).	E-6.3.1			
PW17	The two transfer breakers (in power transfer systems) must be mechanically and electrically interlocked.	E-6.3.1			
PW18	Transfer switches (UL standard 1008) should be used in lieu of paired breakers.	E-6.3.1			
PW19	Provide indicating type control fuses on the front of the switchboard.	E-6.3.1			
PW20	Provide color- coded mimic buses showing power sources, transfer arrangements, essential/nonessential buses, etc.	E-6.3.1			
PW21	Post at the equipment (or have readily available) single line and control schematics.	E-6.3.1			
PW22	Keep circuit breaker racking/ratchet tools, spare fuses, fuse pullers, etc. on hand.	E-6.3.1			
PW23	Clearly label the equipment served by each circuit breaker.	E-6.3.1			
PW24	Provide emergency procedures for AC transfer.	E-6.3.1			
PW25	Train local forces on AC Switchgear to understand procedures and stage occasional rehearsals.	E-6.3.1			
PW26	Provide surge arrestors (TR-NWT-001011) at the AC service entrance of all telco equipment buildings.	E-6.3.1			
PW27	Provide AC tap boxes outside critical central offices to attach a portable engine alternator.	E-6.3.1			
PW28	Design a professionally administered preventive maintenance program for each company's electrical systems.	E-6.3.1			
PW29	Provide a minimum of 3 hours battery reserve for central offices equipped with fully automatic standby systems.	E-6.4.1			
PW30	All new power equipment, including batteries should conform to NEBs.	E-6.4.1			
PW31	When valve regulated batteries are used, provide temperature compensation on the rectifiers.	E-6.4.1			
PW32	A modernization program should be initiated or continued to ensure that outdated equipment is phased out of plant.	E-6.4.1			
PW33	For new installations, multiple smaller battery plants should be used in place of single very large plants serving multiple switches, etc.	E-6.4.1			
PW34	Low voltage disconnects should not be used at the battery plant.	E-6.4.1			
PW35	The rectifier sequence controller should be used only where necessary to limit load on the engine.	E-6.4.1			

Appendix A Service Provider Best Practices Questionnaire

PW36	TelcosService Providers should consider and include the capabilities of smart controllers, monitoring, and alarm systems when updating their power equipment.	E-6.4.1			
PW37	Manufacturers are encouraged to continue to improve the human-machine interfaces of power equipment.	E-6.4.2			
PW38	Provide diverse feeds for SS7 links, BITS clocks, and other duplex circuitry.	E-6.5.5			
PW39	Provide protective covers and warning signs on all vulnerable circuit breakers.	E-6.5.5			
PW40	Ensure that the fuses and breakers meet quality level III reliability.	E-6.5.5			
PW41	Power wire, cable, and signaling cables that meet NEBS should be required in all telecommunications locations.	E-6.5.5			
PW42	Wherever possible, DC power cables, AC power cables and telecommunications cables cable should not be mixed.	E-6.5.5			
PW43	Verify DC fusing levels, especially at the main primary distribution board to avoid over fusing.	E-6.5.5			
PW44	Provide smaller (distributed) power plants closer to the load as part of modernization.	E-6.5.5			
PW45	Detailed methods and procedures are needed to identify all protection required around the energized DC bus.	E-6.5.5			
PW46	Load-test all circuit breakers prior to connecting the load.	E-6.5.5			
PW47	Update installation handbook to include verification of front to rear stenciling.	E-6.5.5			
PW48	Perform high-risk operations at night.	E-6.5.5			
PW49	Procedures and restoral processes are required for any cable-mining job.	E-6.5.5			
PW50	Each company must have an alarm strategy.	E-6.6.3			
PW51	Provide a separate "battery discharge" alarm for all battery plants.	E-6.6.3			
PW52	Redundancy must be provided, so that no single point alarm system failure will lead to a battery plant outage.	E-6.6.3			
PW53	Highlight the battery discharge (and other critical alarms) at the remote center.	E-6.6.3			
PW54	For critical alarms produced by single contacts (one on one), use "normally closed" contacts that open for an alarm.	E-6.6.3			
PW55	Power monitors should be integrated into engineering and operational strategies.	E-6.6.3			
PW56	Maintain the power alarms by testing the alarms on a scheduled basis.	E-6.6.3			
PW57	Provide hands-on training for operation and maintenance of power equipment.	E-6.7.1			

PW58	Place utmost emphasis on the maintenance and response to power alarms.	E-6.7.1			
PW59	Emphasize methods of procedures (MOPs), vendor monitoring and perform risky work at night.	E-6.7.1			
PW60	On removal projects, check for current flow in power cables with AC/DC clamp-on ammeters.	E-6.7.1			
PW61	Provide and test detailed action plans to address emergency situations, such as when both the commercial AC power and the standby engine fails to start.	E-6.7.1			
PW62	Perform annual evaluation/maintenance of all power equipment.	E-6.7.1			
PW63	Run engines annually with all available loads for an extended period, at least 5 hours.	E-6.7.1			
PW64	Use infrared thermographic scanners to check power connections.	E-6.7.1			
PW65	Employ the "Ask Yourself" program to supplement conventional training.	E-6.7.1			
PW66	Vendors should provide clear and specific engineering, ordering, and installation in support of their products.	E-6.8.2			
PW67	Telco Service Provider personnel should evaluate support documentation as an integral part of the equipment selection process.	E-6.8.2			
PW68	Operating personnel m ust be familiar with support documentation provided with the equipment.	E-6.8.2			
PW69	TelcosService Providers should have documented installation guidelines that apply in their company.	E-6.8.2			
PW70	TelcosService Providers should clearly communicate their installation guidelines to all involved parties.	E-6.8.2			
PW71	On-site installation acceptance should include a quality review of conformance to the company's and vendors installation guidelines.	E-6.8.2			
PW72	TelcosService Providers should have procedures for pre-qualification or certification of installation vendors.	E-6.8.2			
PW73	In preparation for a hurricane, place standby generators on line and verify proper operation of all subsystems.	E-6.13			
PW74	In coastal areas, design standby systems to withstand high winds and wind driven rain and debris.	E-6.13			
PW75	Improve fuel systems reliability. Provide redundant pumps for day tanks and a manual-priming pump.	E-6.13			
PW76	Reemphasize the need for local procedures and contingency plans for power emergencies.	E-6.13			
PW77	Provide AC tap boxes outside the central office to facilitate the connection of a portable engine.	E-6.13			
PW78	Remote power monitors are invaluable during and after hurricanes and other power outages.	E-6.13			
PW7	Reemphasize the need for power expertise/power teams.	E-6.13			

9					
PW80	Engineer for fewer but larger remote terminals (RTs) serving larger areas and use bulk power plants instead of distributed power.	E-6.13			
PW81	A significant problem during hurricanes is security from theft of portable generators. Trailer mounted generators equipped with wheel locks are recommended.	E-6.13			
PW82	All future portable generators should be diesel.	E-6.13			
PW83	Better coordination is required with the electric utilities, such as designated local single points of contacts for coordinating restoration.	E-6.13			
PW84	Better methods are required for tracking what is sent into a stricken area, and for loading/unloading generators onto flatbed trucks.	E-6.13			
ES	**Essential Service Best Practices**	**Red Book References**			
ES1	Diverse Interoffice Transport Facilities - When all 9-1-1 circuits are carried over a common interoffice facility route, the PSAP has increased exposure to possible service interruptions related to a single point of failure (e.g., cable cut). The ECOMM Team recommends diversification. diversification of 9-1-1 circuits over multiple, diverse interoffice facilities. Diversification may be attained by placing half of the essential communication circuits on one facility route, and the other half over another geographically diverse facility route (i.e., separate facility routes). Many LECs deploy diverse interoffice facility strategies when diverse facilities are already available	D-6.1.1			
ES2	Diverse Interoffice Transport Facilities with Standby Protection - A variation of the facility diversity architecture is deployment of a 1-by-1 facility transport system. This architecture is protected by a standby protection facility that is geographically diverse from the primary facility. Because no calls are lost while switching to the alternate transport facility during primary route failure, this architecture is considered self-healing.	D-6.1.2			
ES3	Diverse Interoffice Transport Facilities Using DCS - Earlier NRC Focus Group recommendations suggested using diverse interoffice transport facilities from the called serving end office via two diverse Digital Cross-connect Systems (DCS) for concentration. This approach provides diversity and, due to the concentration by the DCS network elements, offers a less costly network solution. Circuit rearrangement activity under this configuration will less likely result in the circuits being placed into non-diverse facilities.	D-6.1.3			
ES4	Fiber Ring Topologies for 9-1-1 Circuits - Fiber optic network elements offer network service providers the ability to aggregate large amounts of call traffic onto one transport facility. Traffic aggregation opposes the diverse facility transport recommendations defined in this document. However, fiber rings permit a collection of nodes to form a closed loop whereby each node is connected to two adjacent nodes via a duplex communications facility. Fiber rings provide redundancy such that services may be automatically restored (self healing), allowing failure or degradation in a segment of the network without affecting service. Fiber rings are used in some metropolitan areas, ensuring essential communications service is unaffected by cuts to fibers riding on the ring. Ring features and functionality are part of the Synchronous Optical Network (SONET) technical requirements.	D-6.1.4			

Appendix A Service Provider Best Practices Questionnaire

	The ECOMM Team believes when essential communications is placed on SONET rings, service interruptions are minimized due to the self-healing architecture employed.				
ES5	Red-Tagged Diverse Equipment - Depending on LEC provisioning practices, the equipment in the central office can represent single points of failure. The ECOMM Team supports the the common LEC practice of spreading 9-1-1 circuits over similar pieces of equipment, and marking each plug-in-level component and frame termination with red tags.The red tags alert LEC maintenance personnel that the equipment is used for critical, essential services and is to be treated with a high level of care.	D-6.1.5			
ES6	Alternate PSAPs from the 9-1-1 Tandem Switch - A common method of handling PSAP-to-Tandem transport facility interruptions is to program the 9-1-1 tandem switch for alternate route selection. If the 9-1-1 caller is unable to complete the call to the PSAP, the tandem switch would automatically complete the call to a pre-programmed directory number or alternate PSAP destination. The alternate PSAP may be either administrative telephones or another jurisdiction's PSAP positions, depending upon the primary PSAPs pre-arranged needs.	D-6.2.1			
ES7	Alternate PSAPs from the Serving End Office - Another method of handling PSAP-to-Tandem transport facility interruptions is to program the end office for alternate route selection. If the 9-1-1 caller is unable to completeto complete the call to the PSAP, the end office switch may automatically complete the call to a pre-programmed directory number or alternate PSAP destination. . The alternate PSAP may be either administrative telephones or another jurisdiction's PSAP positions, depending upon the primary PSAPs pre-arranged needs.	D-6.2.2			
ES8	PSTN as a Backup for 9-1-1 Dedicated Trunks - To ensure that 9-1-1 is minimally affected by potential traffic congestion sometimes experienced in the Public Switched Telephone Network (PSTN), PSAPs commonly create dedicated private public safety networks. A low-cost alternative for handling 9-1-1 calls during periods of failure in the end office-to-9-1-1 tandem transport facility, is to use the PSTN as a backup between the caller's end office and the 9-1-1 tandem switch. Such applications may or may not make use of adjunct devices that monitor primary trunk path integrity. If the primary path to the 9-1-1 tandem switch should be interrupted or all-trunks-busy, the call may be forwarded over the PSTN to a preprogrammed directory number. Further, the caller may be identified if the administrative line is equipped with a caller identification (ID) device.	D-6.2.3			
ES9	Wireless Network as Backup for 9-1-1 Dedicated Trunks - Similar to the PSTN backup for completing 9-1-1 calls when the primary transport facility is interrupted, wireless networks may provide more diversity than the PSTN alternative. (See Figure 6-7) As in Best Practice ES08, an adjunct device may or may not be used to monitor the primary trunk path integrity.	D-6.2.4			
ES10	Intraoffice 9-1-1 Termination to Mobile PSAP - Commonly, the transport facility between the PSAP and the serving end office may not have facility route diversity. To accommodate instances where these facilities are interrupted or it becomes necessary to evacuate the PSAP location, some PSAPs have established mobile PSAP systems that may be connected to phone jacks at the serving end office. The phone jacks, although usually installed inside the end office for security purposes, are typically installed in an accessible location for ease in locating them during an emergency.	D-6.2.5			

	Some PSAPs have prearranged with the serving LEC to permit a jurisdictional employee having an emergency vehicle (e.g., police car) equipped with radio capability to retain a key to the LECs endLECs end office and to connect to an RJ-11 jack forjack for 9-1-1 call interception. . Another type of receptacle may be pre-installed in the end office for connection to a mobile PSAP.				
ES11	Backup PSAP in the LECs Serving Office - Some PSAPs have also prearranged with the serving LEC to house a backup PSAP within the central office.	D-6.2.6			
ES12	Dual Active 9-1-1 Tandem Switches - Dual active 9-1-1 tandem switch architectures enable circuits from the callers serving end office to be split between two tandem switches. Diverse interoffice transport facilities further enhance the reliability of the dual tandem arrangement. Diversity is also deployed on interoffice transport facilities connecting each 9-1-1 tandem to the PSAP serving end office.	D-6.3.1			
ES13	Re-home to backup 9-1-1 Tandem Switch - This architecture is similar to other 9-1-1 tandem switch architectures, but uses more than two 9two-1-1 tandem9-1-1-tandem switches. . A primary 9-1-1 tandem handles a caller's servingcaller's serving end office's emergency calls until a fault occurs. . Interoffice transport facility diversity is attained by splitting interoffice trunks between digital cross-connect systems. PSAP circuits are also provisioned evenly across the 9-1-1 tandem switches, minimizing the single points for failure to occur.	D-6.3.2			
ES14	Redundant Paired 9-1-1 Tandems - In redundant/paired tandem switch applications, half of the 9-1-1 circuits are connected to eachto each 9-1-1 tandem switch. . If event call handling capabilities in one of the 9-1-1 tandem switches are interrupted, standard hunt group features in the caller's serving end office switch will select a call path via the other 9-1-1 tandem switch. Although the redundant/paired tandem configuration requires the complexity of maintaining identical routing data on both 9-1-1 tandem switches, the automated re-selection of an alternate call path enables call completion without manual intervention. . Therefore, this network arrangement is more effective during momentary network failures.	D-6.3.3			
ES15	Multiple Diverse Tandem Switches with Diverse DCSs - In a multiple tandem switch application, a backup tandem switch is available to handle 9-1-1 calling in the event the primary 9-1-1 tandem switch fails. Upon detection of failure of the primary 9-1-1 tandem, network controls may be activated by remote or local network surveillance forces that will steer 9-1-1 calling to the backup 9-1-1 tandem switch. Such steering may be accomplished through use of digital cross-connect elements available in many LEC end offices.	D-6.3.4			
ES16	TOPS as a 9-1-1 Tandem Backup - Operator services tandem switches can also serve as backup and/or overflow for network elements, due to their ubiquitous connectivity throughout the telephone network. In most instances, existing trunking and translations may be used when adding a Traffic Operator Position System (TOPS) to the 9-1-1 network. When an interoffice transport facility fails or an all-trunks-busy condition occurs, the backup/overflow route to the operator services tandem is selected. The operator tandem switch recognizes the call as an emergency by translating the 9-1-1 dialed digits, and may be preprogrammed to automatically route the call to the serving 9-1-1 tandem switch.	D-6.3.5			

Appendix A Service Provider Best Practices Questionnaire

	Further, if the operator tandem switch is unable to access the 9-1-1tandem switch, the call will automatically be “looped around” so that an operator may manually answer the call and manually attempt to reach emergency services providers.				
ES17	Reverse Trends toward Centralization - Network service providers should move to eliminate single points of failure in the interoffice facilities, 9-1-1 tandem switches and ALI data base portions of the public switched network. Measures include exploiting existing facility route diversity, reversing a trend towards concentration of large numbers of PSAPs on individual 9-1-1 tandem and deploying redundant, diverse ALI systems over diverse facilities. Tandem switches used for 9-1-1 call routing are considered critical to a jurisdiction’s ability to respond to emergency calls. Some of these switches connect over one million telephones, enabling access to the appropriate Public Safety Answering Point (PSAP). Although the 9-1-1 tandem switches are usually deployed as redundant architectures, some software or procedural errors could interrupt the ability to complete the primary call path for 9-1-1 callers. To minimize the impact of such events, the ECOMM Team endorses deploying either multiple or redundantor redundant/paired tandem switches in 9-1-1 network architectures.	D-6.4			
ES18	Local Loop Diversity - The local loop access is defined as that portion of the network which connects the caller (i.e., the subscriber or the PSAP) to the network serving end office. The local loop is potentially a single point of failure. Although it is unlikely the subscriber will purchase diverse transport facilities for typical PSTN service, the ECOMM Team recommends that PSAP local loops be diverse where possible and/or make use of wireless technologies as a backup for local loop facility failure (e.g., cable cuts)	D-6.5			
ES19	Network Management Center and Repair Priority - The ECOMM Team recommendsthat network management centers (NMCs) remotely monitor and manage the 9-1-1 network componentsThe NMCs should use network controls where technically feasible to quickly restore 9-1-1 service and provide priority repair during network failure events.	D-6.6			
ES20	Diverse ALI Data Base Systems - The ECOMM Team recommends that ALI systems be deployed in a redundant, geographically diverse fashion (i.e., two identical ALI data base systems with mirrored data located in geographically diverse locations). Deployment of fully redundant ALI data base systems, such that ALI system hardware and/or software failure does not impair ALI data accessibility, will furtherwill further improve ALI reliability. . When deployed with geographically diverse transport facilities, single points of failure may be eliminated. The NRC also recommends placement of the ALI data on fault-tolerant computer platforms to increase the reliability of ALI display retrievals. Finally, “hot spare” computers should be held in reserve for catastrophic events.	D-6.7			
ES21	Move Mass Calling Stimulator away from 9-1-1 Tandem Switch - Mass calling events may cause 9-1-1 service interruptions. . Service interruptions caused by media stimulated calling has prompted the LECs to reassess and improve the handling of mass calling events. The 9-1-1 Tandem switch serves as the most	D-6.8.1			

Appendix A Service Provider Best Practices Questionnaire

	critical network element in providing 9-1-1 service. If a media stimulated mass calling event is served by the 9-1-1 Tandem, the PSAPs being served by the 9-1-1 Tandem may experience delayed dial tone when call transfer is attempted by the PSAP personnel. The PSAP may also experience delays in call completion (ring-back tone) or a fast busy signal, which indicates that the call has failed to complete. To mitigate such instances,the ECOMM Team recommends moving high volume call events to another end office or foreign exchange.				
ES22	Pre-Planning for Mass Calling Events - To minimize the potential of interruption caused by media driven mass calling events, the LEC can identify periods of low call volume traffic so that the media may schedule mass calling events during low traffic periods. The ECOMM Team supports such efforts by the LECs, andand suggests that LEC external affairs and marketing groups work closely with media organizations to ensure 9-1-1 callers are unaffected by mass calling events.	D-6.8.2			
ES23	Contingency Plan Development - Contingency plan development is the process of planning for recovery from a disaster that could impact the critical functions of a business operation. Disaster recovery planning involves: ? Advance planning and arrangements necessary to ensure continuity of critical business functions. ? Making sufficient agreed-upon preparations and designing and implementing a sufficient set of agreed-upon procedures for responding to a disaster event. ? Implementing procedures that will either deter or reduce the business risk of previously identified threats. ? Developing a plan w hichplan, w hich covers events that could result in the total or partial losspartial loss of operational capability or destruction of a physical facility. ? Developing a plan w hichplan, w hich includes procedures and availability of critical equipment and personnel for automated and manual functions. The service provider has the responsibility to ensure continuity of service to the PSAP. (For more detail on this Best Practice, click on the **More Detail Worksheet.)**	D-6.9.1			
ES24	Contingency Plan Training - Once a contingency plan is developed, it should be periodically tested. These tests can be of various types: ? Desktop check tests (using a check listchecklist to verify familiarity of "what to do in case of"). ? Procedures verification test (verify that established procedures are followed in a simulation). ? Simulation test (similar to a fire drill, e.g., simulating a disaster and monitoring themonitoring the response). ? Actual operations test (cause an event to happen, e.g., pow er or computer failure and monitor the response). The importance of testing a contingency plan is critical to its success. An annual schedule of testing and evaluating written results is an excellent method of ensuring that a plan will work in the event of a disaster and for identifying weaknesses in the plan. Close cooperation between a service provider and the PSAP in conducting actual operations testing will be of mutual benefit to both the service provider and the PSAP. An annual comprehensive operational test of the contingency plan is strongly encouraged.	D-6/9/2			
ES25	Public Education on Proper Use of Essential Communications - The public's proper use of 9-1-1 service is critical to the effectiveness of the emergency network's operation. Misuse of 9-1-1 could lead to the following: ? Congestion of the 9-1-1 network, leaving callers with real emergencies unable to contact a 9-1-1 operator. ? Exhaustion of resources on non-emergency situations. ? Reduction in a jurisdiction's ability to respond to emergency	D-6.9.3			

	situations in a timely manner because of the jurisdiction's emergency response agencies being overwhelmed by responses to non-emergency situations. This could have potentially disastrous effects on the public's perception of its emergency network and emergency response agencies. (For more detail on this Best Practice, please click on the **More Detail Worksheet.)**					
ES26	Improve Communications among Network Providers and PSAPs - Network service providers, 9-1-1 administrators, and public safety agencies should continually strive to improve communications among themselves. They should routinely team to develop, review, and update disaster recovery plans for 9-1-1 disruption contingencies, share, share information about network and system reliability, and determine user preferences for call overflow routing conditions. They should actively participate in industry forums and associations focused on improving the reliability of emergency services and the development of technical industry standards. The National Emergency Number Association (NENA) and theand the Association of Public-safety Communications Officials (AP CO) are just two of the organizations that are open to all stakeholders of 9-1-1 service delivery and that are focused on finding 9-1-1 solutions for emerging technologies (e.g., wireless, PBX, ALEC).	D-6.10				
ES27	Common Channel Signaling (CCS) - The ECOMM Team considers ll of the Best Practices formerly defined by the earlier NRC effort as still being valid, with the exception of the former NRC recommendation to avoid use of the CCS network for 9-1-1 services. The CCS network has demonstrated reliability for non-emergency applications, and may now be considered as a viable alternative for emergency network routing applications. Further, telecommunication standards bodies are exploring creation of SS7 compatible data packets for passing caller location and other wireless information detail to Integrated Services Digital Network (ISDN) PSAPs.	D-6.11				
ES28	Critical Response Link Redundancy/Diversity - The ECOMM Team recommends that the redundancy and diversity concepts set forth in section 6.1 (Defensive Measures for Interoffice Facilities) be applied to other network links considered vital to a community's ability to respond to emergencies. Types of links that are critical to the provision of emergency aid include communication links from the PSAP location to: ? Law enforcement dispatchers and/or response personnel. ? Emergency medical service (EMS) dispatchers and ambulance response units. ? Fire fighter dispatchers and response personnel. ? Poison control centers and other agencies offering remote diagnostic information and advice on how to respond to requests for emergency aid. ? Trauma centers and similar emergency hospices. Standards must be established to address interconnection issues between PSAP and CMRS/cable television service providers.	D-6.12				
ES29	Media and Repair Link Redundancy/Diversity - The ECOMM Team recommends that the redundancy and diversity concepts set forth in section 6.1 (Defensive Measures for Interoffice Facilities) be applied to network links considered vital to a community's ability to respond to emergencies. Types of links that are critical to the provision of emergency aid during such events include communication links from the PSAP location to broadcast media organizations and local network provider repair centers. Media organizations can alert the public during periods of emergency network degradation or outage through appropriately worded public service announcements, relieving excessive call volumes, and making the public aware of interim emergency aid access alternatives .	D-6.13				

	In addition, dedicated network links and/or alternate accesses to network provider repair personnel will ensure that interruptions are known immediately and that repair personnel are mobilized expeditiously.				
ES30	Private Switch/Alternative LEC ALI - The ECOMM Team supports inclusion of ALI data for alternate providers (PSALI, ALEC ALI, etc.) in the ALI systems, and urges the FCC to aggressively pursue closure on those issues remaining for Docket 94-102, and to require affected service providers to participate in PSAP PSALI programs. PSAPs have become increasingly reliant on the ALI data administered by the LECs, and believe that those individuals served by private telecommunication providers and/or alternate LEC providers should have their a ddress information contained in their ALI data base systems. The NENA Recommended Formats for Data Exchange and the NENA Recommended Protocols for Data Exchange were established to enable ALI data integration of these providers.	D-6.14			
ES31	CMRS - Emergency Calling - The ECOMM Team recommends that the CMRS industry consider 9 -1-1 as the standard access code for emergency services, such as law enforcement, fire, EMS. Implementation of such a standard would eliminate confusion among mobile communicati ons users when they are in a roaming mode.	D-6.15			
ES32	Cable Television Services - The cable television industry has published a document titled NCTA Recommended Practices for Measurement on Cable Television Systems. This document is available from NC TA. The document is technically oriented for systems engineers. Based on information obtained from NCTA, the ECOMM Team recommends that the NCTA document form the basis for cable television services best practices. This will create a more reliable environment for all services, including emergency communications.	D-6.16			
ES33	Outage Reporting - The ECOMM Team recommends that all providers of essential communications have a uniform method of reporting and tracking significant service outages for internal use and, where required, for outage reporting to the FCC. Root cause analysis, publication of results and new best practices may be left up to the industry.	D-6.17			
PR	**Procedural Best Practices:** The following Best Practices address PRocedures. They areThey associatedare associated with the installation, maintenance, and administration of Network Elements involved in call routing and or transportadministration of Network Elements involved in call routing and or transports (e.g., circuit switch, packet switch, routers, ATM, ATM/FR nodes, STPs, SCPs, DCS, SONET Nodes, WDM Nodes, and DLC).				

Appendix A Service Provider Best Practices Questionnaire

PR01	Awareness Training (Replaces SN-01 DX01)- There is a critical need for a broad based educational system for all field and management personnel involved in the operation, maintenance, and support of Network Elements. The Awareness Training must stress the importance of end to end communications for all persons involved in maintenance activities on these systems. A successful program must educate its target audience on the technology, its benefits and risks, and the magnitude of traffic carried. The training must emphasize the functionality and the network impact of failure of active and standby (protect) equipment in processors, interfaces, peripheral power supplies, and other related componentsand the identification of active and standby (protect) units. Special emphasis should focus on the systematic processes for trouble isolation and repair.	B-5.2.4.5, D-6.1.1			
PR02	Technical Training (Replaces SN-04, SN-11, DX-28) - Service providers should establish a minimum set of work experience and training courses which must be completed before personnel may be assigned to perform maintenance activities on network elements, especially when new technology is introduced in the network... This training must stress a positive reinforcement of procedures at all times. The use of signs designating various work areas, labels on equipment and cabling, properly identified inventory storage areas, log sheets for work performed, and procedures to be followed in case of emergencies. This training must also emphasize the steps required to successfully detect problems and to isolate the problem systematically and quickly without causing further system degradation. Special emphasis should be placed on maintaining and troubleshooting problems related to system power equipment which can add significant delay to restoration activities.	B-5.2.5.4, B-5.2.8, D-6.2.11			
PR03	MOPs and Acceptance/Verification Check-Off Sheets for Hardware and Software Growth/Change Activities(Activities (Replaces SW-02, DX-25, DX-04)- Methods- Methods of procedure (MOPs) should be prepared for all hardware and software growth and change activities. As far as practicable, the MOP should be prepared by the people who will perform the work. The MOP should be approved by the responsible engineer, line operations manager, installation manager, and others, as appropriate; and deviations from the documented process should also be approved by this team. When it is necessary to reference other documents in the MOP, these references should be detailed and include appropriate issue/date information. The MOP should identify each step required to perform the work. As each work function is completed, it should be signed off in the MOP. An acceptance/verification testing check-off sheet should also be utilized to assure that the work activity was performed correctly.	C-5.1.3.3, D-6.2.4			
PR04	Information Sharing Guidelines (Replaces SN-13) - Industry Guidelines for the Sharing of Information which could lead to network outagesInformation, which could lead to network outages, is included in the NIIF Reference document Part VII.Part VII. This document is intended to provide the appropriate guidance to facilitate the sharing of information. It identifies types of information whichinformation, which may be shared, the circumstances under which it should be shared, the extent to which sharing is appropriate, and the mechanisms and timing for that sharing. It represents industry consensus arrived at with the full participation of members of the Network Interconnection Interoperability Forum which consists of Access Service Providers, Access Service Customers and Vendor/Manufacturers.	B-6.1.2			
PR05	Centralized Control for DCSs (Replaces DX-02) - It is recommended that service providers provide centralized	D-6.1.1			

	maintenance, administration, surveillance and support for all network elements. Monitoring and control should be in as few places as possible to provide consistency of operations and overall management.				
PR06	Training in Trouble Detection and Isolation (formerly SN-10) - Lack of troubleshooting experience and proper training in this area usually prolongs the trouble detection and isolation process. It is recommended that network operators be adequately trained in the trouble detection and isolation process.	B-5.2.8			
PR07	Outage Information Sharing - A prime source for information concerning outages is the network outages reported to the FCC as required by Section 63.100 of the rules. Final reports of all 1999 outages are posted at www.fcc.gov/Bureaus/Engineering_Technology/Filings/Network_Outage/1999/report.html. The final reports for 1996, 1997, and 1998 are also available simply by changing the year in the above URL. The posted reports are Adobe Acrobat .pdf (portable document format) scans of the reports provided by the carriers. Review of the reports will enable the reader to become aware of significant problems impacting the network.	B-6.1.2			
PR08	Maintaining Link Diversity (replaces SN-07) - Industry Guidelines for Maintaining Link Diversity can be found in the NIIF Reference Document, Part III, Attachment G. The following are some of the Operating Principles of the document: Link diversification validation should be performed at a minimum of twice a year, at least one of those validations shall include a physical validation of equipment compared to the recorded documentation of diversity. ? The validation of diversification is the responsibility of every network service provider that provides or utilizes SS7 links. ? Limitations on diversification should be considered at the time of deployment, such limitations may consist of, geography, facilities, circuit design and tariffs.	B-5.2.7.1.1, B-6.2.1			
PR09	Off-Peak Scheduling (Formerly SN-03) - High risk, potentially service affecting maintainancemaintenance and growth procedures should be scheduled during weekend and off-hours.	B-5.2.4.5			
PR10	Review Rehome Procedures - Network service providers carefully review all rehome procedures and undertake meticulous pre-planning before execution. Communication to all inter-connected networks will be essential for success in the future. It is also important to make sure that rehome procedures are carefully followed.	B-5.2.8			
PR11	Review Detection & Manual Intervention Procedures - Network operators should be adequately trained in (1) detection of conditions requiring intervention, (2) escalation procedures, and (3) manual recovery techniques.	B-5.2.8			
PR12	Develop Crisis Management Exercises (Formerly SN-15) - During the past several years a number of disastrous events, the Oklahoma City bombing, the Midwest flooding, earthquakes in California and hurricanes in Louisiana, Florida and Hawaii, have prompted an increased awareness on the part of all members of the telecommunication industry to the critical need to have a Disaster Preparedness strategy. . This strategy should outline a network service provider's Disaster Preparedness organization, the roles, responsibilities and training of its members and provide for cooperative interaction among both internal and external	B-6.2.2			

	organizations. The purpose of this strategy is to provide for the development of emergency plans that protect employees, ensure service continuity and provide for the orderly restoration of critical services in the event of a major network catastrophe.				
PR13	Test a Network's Operational Readiness through planned drills or simulated exercises. Service Providers should conduct exercises periodically keeping the following goals in mind: ? The exercise should be as authentic as practical. Scripts should be prepared in advance and team members should play their roles as realistically as possible. ? While the staff must be well prepared, the actual exercise should be conducted unannounced in order to test the responsiveness of the team members and effectiveness of the emergency processes. Also, callout rosters and emergency phone lists should be verified. ? Early in the exercise, make sure everyone understands that this is a disaster simulation, not the real thing! This will avoid unnecessary confusion and misunderstandings that could adversely affect service. ? It is particularly important to coordinate disaster exercises with other Service Providers and vendors. ? It is very important immediately following the drill to critique the entire procedure and identify				
PR14	Validate Upgrades, new procedures and commands in Lab Environment (Formerly DX-05 and DX-07) All Service Providers should establish and document a process to plan, test, evaluate and implement all major change activities onto their network. This industry best practice describes a process that should include: ? The establishment of a multi-discipline core team, which includes suppliers, to plan and implement changes. The team's focus should be on planning, testing, and evaluation of all major network elements and systems ? The validation of all upgrades and procedures in a lab environment prior to the first application in the field. ? The creation of a "Methods of Procedure (MOP)" for each change activity that outlines the maintenance steps to be taken and an emergency restoration plan. Finally, it is highly recommended that, in response to the ever-increasing amount of change activity being performed, each Service Provider establish a "Change Management Control" (CMC) group to act as a customer advocate. (	D-6.1.2			
PR15	Restrict Commands Available to Technicians	D-6.1.3			
PR16	Ensure Facility & DCS Databases in Sync	D-6.1.3			
PR17	Initiate Procedures to Review Passwords	D-6.1.3			
PR18	Establish Procedure to Uninhibit Alarms after Provisioning (Formerly DX-14) - The volume of alarms during provisioning create a potential for alarm saturation and makes it very difficult to differentiate between a real alarm and those caused by other activities. A common practice is to simple inhibit these alarms or set their thresholds so high they do not report. The danger here is that there must be a fail-safe measure to turn these alarms back on when the facility is carrying traffic.	D-6.1.3			
PR19	Schedule System Backups (Formerly DX-22) - All Service Providers should establish policies and procedures that outline how critical network element databases, (e.g. digital cross connect system databases, switching system images), will be backed up onto a storage medium (tape, optical diskettes, etc.) on a scheduled basis. These policies and procedures should address, at a minimum, the following: ? Database backup schedule and verification procedures ? Storage medium standards ? Storage medium labeling ? On site and off site storage	D-6.1.8			

	? Maintenance and certification ? Handling and disposal The implementation of this practice will mitigate the impact of data corruption or some other loss of a critical network database.				
PR20	Companies should appoint a Synchronization Coordinator for their company who will perform the responsibilities contained in SR-TSV-002275. Companies should provide the name of their Synchronization Coordinator to the NIIF for inclusion in its Companyits Company Specific Contact Directory.	B-5.1.2.5, B-5.2.2.5, B-5.3.2.5, B-5.4.2.5			
PR21	Companies should comply with the synchronization standards addressed in the ANSI Standard T1.101, entitled "Digital Network Synchronization"	B-5.1.2.5, B-5.2.2.5, B-5.3.2.5, B-5.4.2.5			
PR22	Bilateral agreements should be established between interconnecting network providers in accordance with the bilateral agreement template contained in Section 5.6.	B-5.1.3.1			
PR23	Bilateral agreements between interconnecting networks should address the issue of fault isolation. At a minimum, these agreements should address the escalation procedures to be used when a problem occurs in one network. Second, the agreement should address which company will be in charge for initiating various diagnostic procedures. Finally, the agreement should address what information will be shared between the interconnected companies.	B-5.1.3.3			
PR24	To keep overflow traffic conditions from adversely affecting interconnected networks, interconnected network providers should utilize network surveillance and monitoring. In addition, companies should follow the guidelines for advanced notification of media-stimulated call-in events as outlined in Partin Part 6 of the NIIFthe NIIF Reference Document concerning Media Stimulated Call-in Events. . Further, interconnecting companies should include a contact name for inclusion in the Company Specific Contact Directory. Finally, interconnecting companies should address the control of overflow conditions in their bilateral agreements.	B-5.1.3.5, B-5.4.3.5			
PR25	Information sharing should be utilized by all network providers to minimize recurrence of service disruptions. . The guidelines contained in the NIIFthe NIIF Reference Document can be used for this purpose. . Additional requirements for the sharing of information between interconnected companies should be addressed in bilateral agreements.	B-5.1.6			
PR26	New entrants should, at a minimum, have a communications structure in place for timely notification of affected parties in the event of disasters or emergencies.	B-5.1.3.7			
PR27	Companies should appoint and provide the name of a Mutual Aid Coordinator to the NIIFthe NIIF for inclusion in the Companythe Company Specific Contact Directory, which is published on a bi-annual basis.	B-5.1.3.7			

Appendix B Supplier Best Practices Questionnaire

	NRIC II Supplier Best Practices Questionnaire				
	Please enter your company name:				
	Name of contact person: Phone No.:				
ID	**Recommendation**	*Purple* **Book Reference**	**Implementation (E-Everywhere, NE-Nearly Everywhere C-Critical Places Only, F-Few Places, N-Nowhere)**	**Effectiveness Rating (1- 5) (0-Don't Know)**	**Relative Cost to Implement (VL, L, M, H, VH)**
SP01	Software Fault Insertion	B-5.2.4.5, 5.2.5.4.			
SP02	Hardware Fault Insertion	B-5.2.4.5, 5.2.5.4.			
SP03	Review of Fault Recovery Actions	B-5.2.4.5, 5.2.5.4.			
SP04	Minimize Initialization Durations	B-5.2.4.5, 5.2.5.4.			
SP05	Place Added Emphasis on Human Factors Design	B-5.2.7.1.1			
SP06	Failure Data Collect. & Root Cause Analysis	B-6.1.1			
SP07	Enhance System Defensiveness to Service Affecting Activity	C-5.1.3			
SP08	Reduce Need for Scheduled Outages	C-5.2.3(1-4)			
SP09	Hardware & Software Fault Recovery Design Convergence	C-5.3.3(5-6))			
SP10	Enhance Software Development Methodology	C-5.4.3(1-10)			
SP11	Collaboration on Root Cause Analysis	D-6.1.1			
SP12	Establish Core Team to Plan, Test and Evaluate Change Activities	D-6.1.2			
SP13	Validate Upgrades in Lab Environment	D-6.1.2			
SP14	Eliminate Silent Failures	D-6.1.4, 6.1.8			
SP15	Establish Performance Levels	D-6.1.6			
SP16	Ensure Adequate Documentation	D-6.2.1, 6.2.2, 6.2.3			
SP17	Establish Change Control Database	D-6.2.3			
SP18	Document System Overview & Procedures	D-6.2.4			
SP19	Develop Acceptance Testing Checkoff Sheet	D-6.2.4			
SP20	Include Troubleshooting Flowcharts in Documentation	D-6.2.4			
SP21	Use Human Factors Considerations in Documentation Development	D-6.2.5			

SP22	Develop Training for Customer Needs with Customer Testing	D-6.2.7			
SP23	Update Training as Product Evolves	D-6.2.8			
SP24	Develop Training for Local & Centralized Tier 1/ 2 OAM&P Personnel	D-6.2.9, 6.2.10			
SP25	Improve Software Process	D-6.3			
SP26	Review Level of Inspection on Critical Components	D-6.4.1(a)			
SP27	Deploy Systems with Redundant Disk Drives	D-6.4.1(c)			
SP28	Improve Documentation on Backup & Recovery	D-6.4.1(d)			
SP29	Develop Redundant Controller Architecture	D-6.4.2(a)			
SP30	Develop Better Automatic Congestion Control Mechanism	Red Book Section III-5.6			

Appendix C Facilities Best Practices Questionnaire

Facilities Solution Team Best Practices Questionnaire												
Please enter your company name:												
Name of contact person:									Phone No.:			
			Categories			**Implementation**					**Value**	
ID	Focus Team	**Recommendation**	**Obsolete? (Y -Yes N -No)**	**Too General? (Y -Yes N -No)**	**Relative Cost to Implement (VL, L, M, H, VH)**	**E - Everywhere, NE - Nearly Everywhere, M - Only For Major Routes I - Isolated or Rare, N - Nowhere**	**Planned to Implement (Y,N)**	**Alternate Solution (Y,N)**	**Implement. of Alternate Solution (E,NE,M,I,N)**	**Explanation of Alternate Solution**	**Effective-ness Rating (1- 5) (0-Don't Know)**	**Effective-ness Rating (1- 5) Of Alter-native**
1	Fiber	Adherence to Procedures										
2	Fiber	Warning Tape - place tape 12 in. above the cable										
3	Fiber	Visible Cable Markings										
4	Fiber	Respond Quickly to Locate Requests										
5	Fiber	Accurate Locates										
6	Fiber	Enhanced Locating Equipment - use current, and/or emerging technologies										
7	Fiber	Use of Plant Route Maps - secondary checking of plant drawings relative to marking										
8	Fiber	Hand Dig in Safety Zone										
9	Fiber	Technician Supervision - assign technical personnel to observe activties at work sites where digging is underway										
10	Fiber	On-Line Technical Support - centralized support for technicians										
11	Fiber	Cooperation With Contractors -easy access, open communications with contractors										
1	Fiber	Training - continuous refresher										

2		training										
13	Fiber	Contractor Awareness - public service seminars, literature and announcements										
14	Fiber	Contact With Land Owners - proactively eductate and communicate with right-of-way owners										
15	Fiber	Patrol Cable Routes										
16	Fiber	Audits/Surveys of Plant - periodically check and validate outside plant records and data										
17	Fiber	Barriers - place barriers around poles and above ground structures										
18	Fiber	Buried Cable - bury fiber cable in accordance with standards										
19	Fiber	Buried Facilities - bury structures out of sight and to appropriate depths										
20	Fiber	Shielding										
21	Fiber	Protective Devices - use rodent devices on poles and cable sheaths in rodent infested areas										
22	Fiber	Stronger Conduit - use reinforced PVC pipe in rodent infested areas										
23	Fiber	Separate Pole Lines - avoid joint use utility poles with fiber optic cable if justified by cost/benefit										
24	Fiber	No Visible Markings - avoid use of visible markings in areas prone to vandalism										
25	Fiber	Secured Manholes - use lockable mandhole covers in areas prone to vandalism										
26	Fiber	Ventilate Manholes - install automatic purging devices in contaminated manholes										
27	FST-1	Pass comprehensive state one-call legislation										
28	FST-1	Increase industry coordination and cooperation on federal and state one-call legislation efforts										

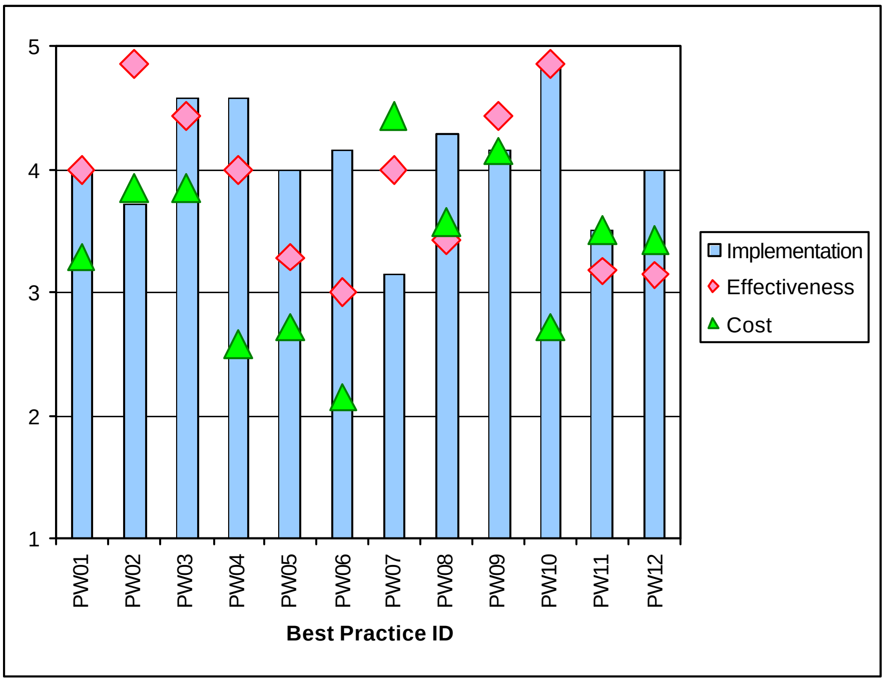
		one-call legislation efforts										
29	FST-1	Establish a dedicated Cable Damage Awareness/Prevention Program with excavators, locators, and municipalities										
30	FST-1	Identify critical routes and provide these routes with additional protection										
31	FST-1	Promote the development of industry standard markings										
32	FST-1	Establish training, qualification and performance evaluation of internal and external utility locators										
33	FST-1	Design and place new facilities to minimize risk; use subsurface utility engineering										
34	FST-1	Provide physical diversity on critical routes when justified by a thorough risk/value analysis										
35	FST-1	Play active role on One-Call Board										
36	FST-1	Jointly relocate facilities										
37	FST-1	Employ courtesy or mutual right of way jeopardy notification										
38	FST-1	Evaluate the performance of contracted excavators against internal performance										
39	FST-1	Implement a rapid restoration program with quick, easy access to records										
40	FST-1	Implement a rapid restoration program aimed at reducing time to locate faults										
41	FST-1	Provide the communication and equipment access needed for a rapid restoration program										
42	FST-1	Implement a rapid restoration program with faster and better dispatch										
43	FST-1	Implement a rapid restoration program with comprehensive site preparation										
44	FST-1	Provide the tools to implement a rapid restoration program										

4												
45	FST-1	Provide fast splicing as part of the rapid restoration program										
46	FST-1	Assess and implement most of the DCS Focus Group's Recommendations when operating large SONET/ATM ADM's										
47	FST-1	Take additional precautions when deploying SONET OC-192 or 10G bit/sec ADMs or DCSs										
48	FST-2	Track and analyze facility outages using the new categorization of facility outages. Take action if any substantial negative trend arises or persists.										
49	FST-2	Reestablish the Cable Electronics Subteam to determine ways to reduce the number and impact of cable electronics outages.										
50	FST-2	Follow the excavator best practices described in the Minimum Suggested Damage Prevention Guidelines - Excavation Procedures for Underground Facilities.										
51	FST-2	Conform to the Minimum Performance Guidelines for One-Call Notification Systems.										
52	FST-2	Conform to the Minimum Guidelines for Facility Owners.										
53	FST-2	Conform to the Guidelines for Prospective Excavation Site Delineation and Location Markout.										
54	FST-2	Pass comprehensive federal One-Call legislation by both Houses of Congress.										
55	FST-2	Maintain the ATIS/NRSC Facilities Solution Team for the Next Year to Act as the Focal Point for Follow-Up.										

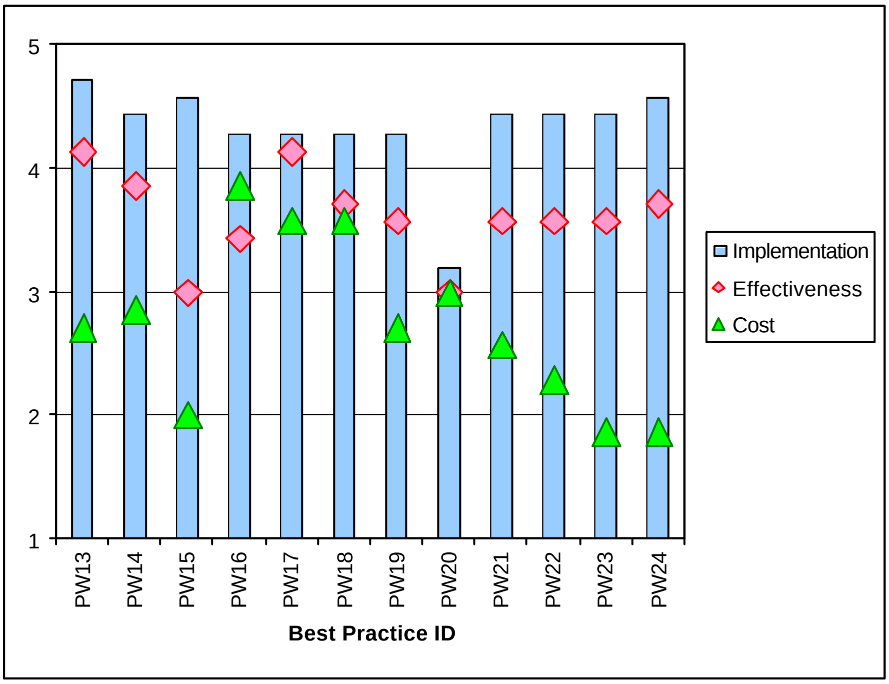
Appendix D –Service Provider Best Practice Questionnaire Results

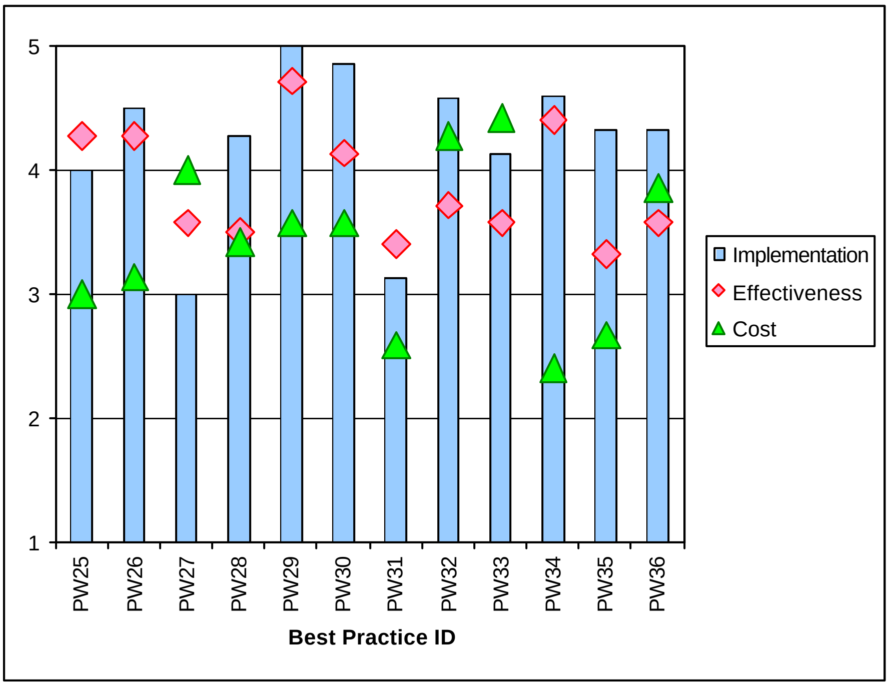
This Appendix provides the graphs which indicate how each of the "old" Best Practices was rated on effectiveness, implementation, and cost. This Appendix provides results for the Service Provider Best Practice Questionnaire that is listed in Appendix A. A high number for effectiveness indicates that the respondents believed that this Best Practice was highly effective in preventing outages. A high number for cost indicates that this Best Practice is very costly to implement (relative to other potential Best Practices). A high number for implementation indicates that this Best Practice is implemented everywhere.

The following six charts show the average rating of the Power Best Practices in terms of effectiveness, implementation, and cost (see the questionnaire in Appendix A for a description of these Best Practices). These Best Practices apply to Service Providers.

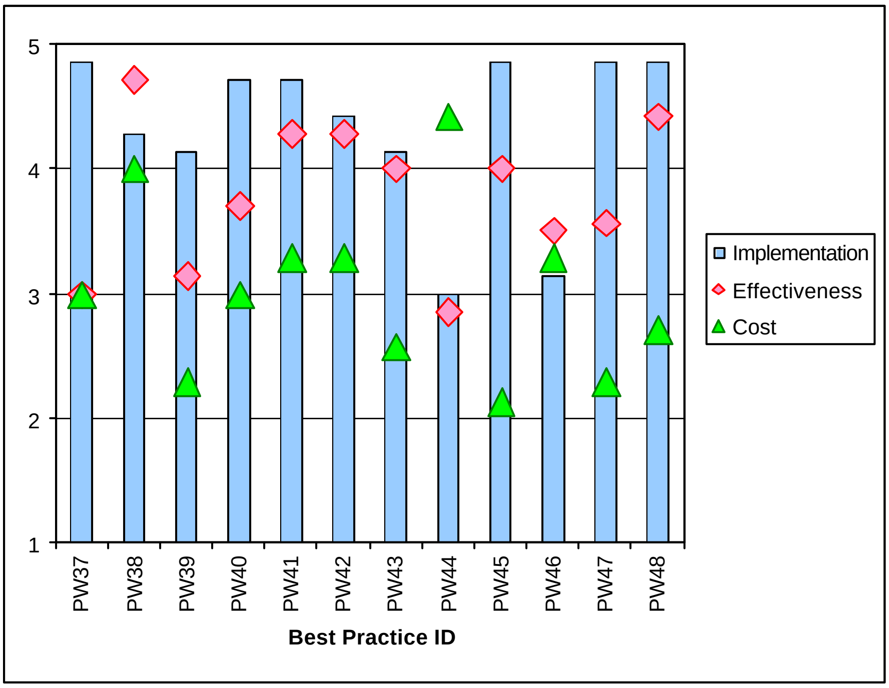


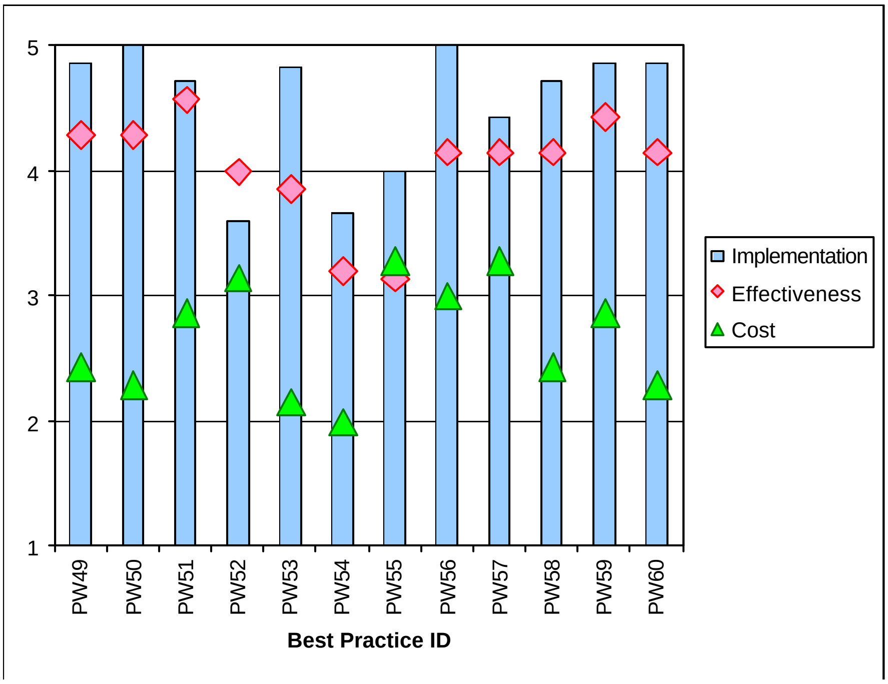
Appendix D –Service Provider Best Practice Questionnaire Results



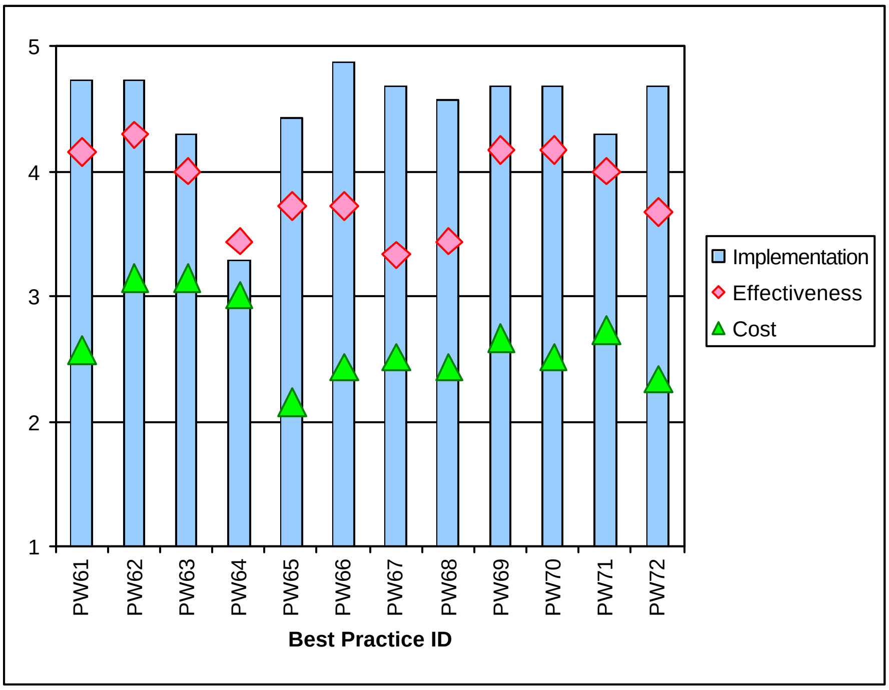


Appendix D –Service Provider Best Practice Questionnaire Results



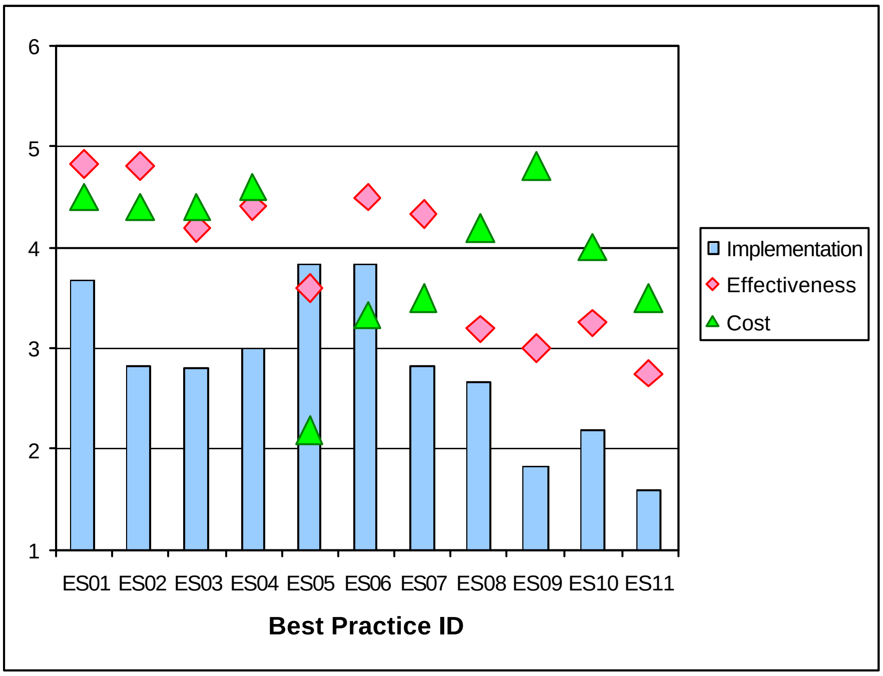


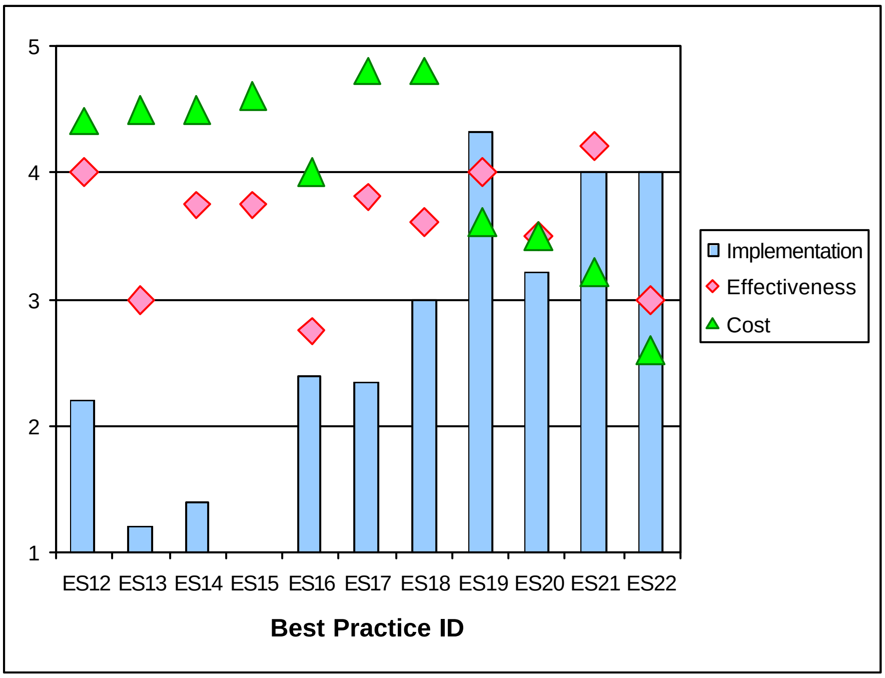
Appendix D –Service Provider Best Practice Questionnaire Results



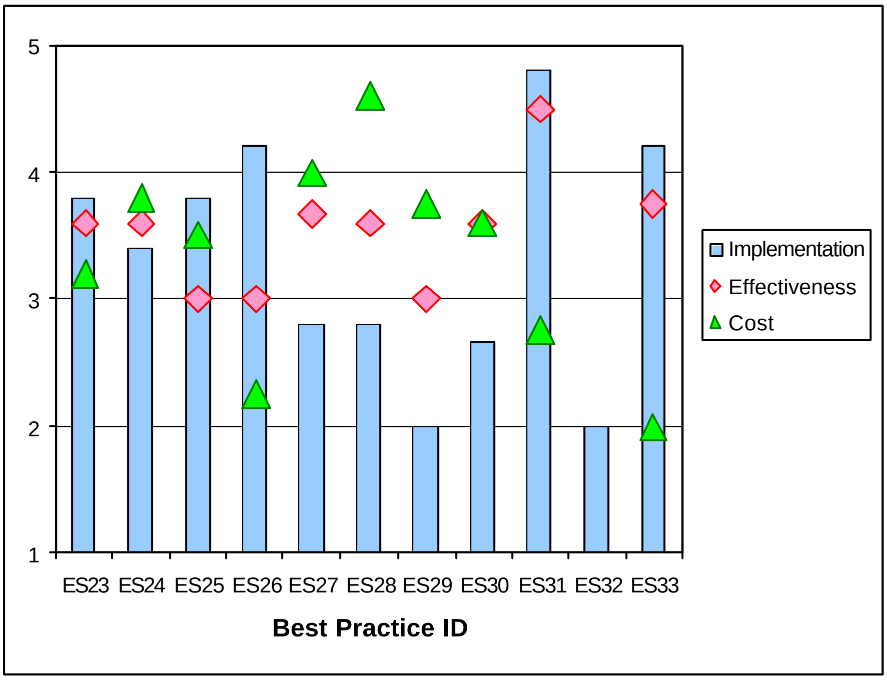
The following three charts show the average rating of the Essential Services Best Practices in terms of effectiveness, implementation, and cost (see the questionnaire in Appendix A for a description of these Best Practices). These Best Practices apply to Service Providers.

Appendix D –Service Provider Best Practice Questionnaire Results



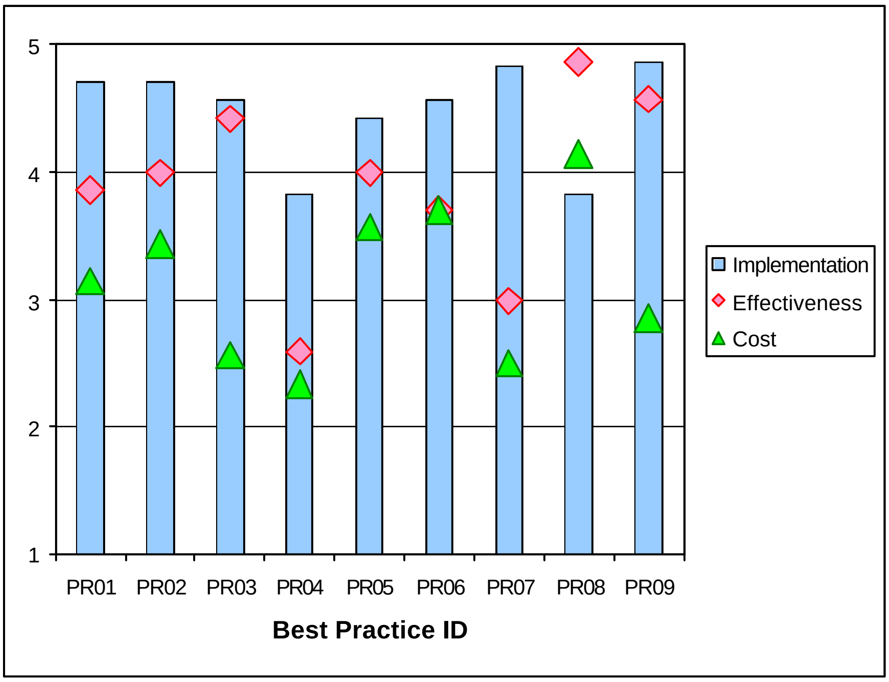


Appendix D –Service Provider Best Practice Questionnaire Results

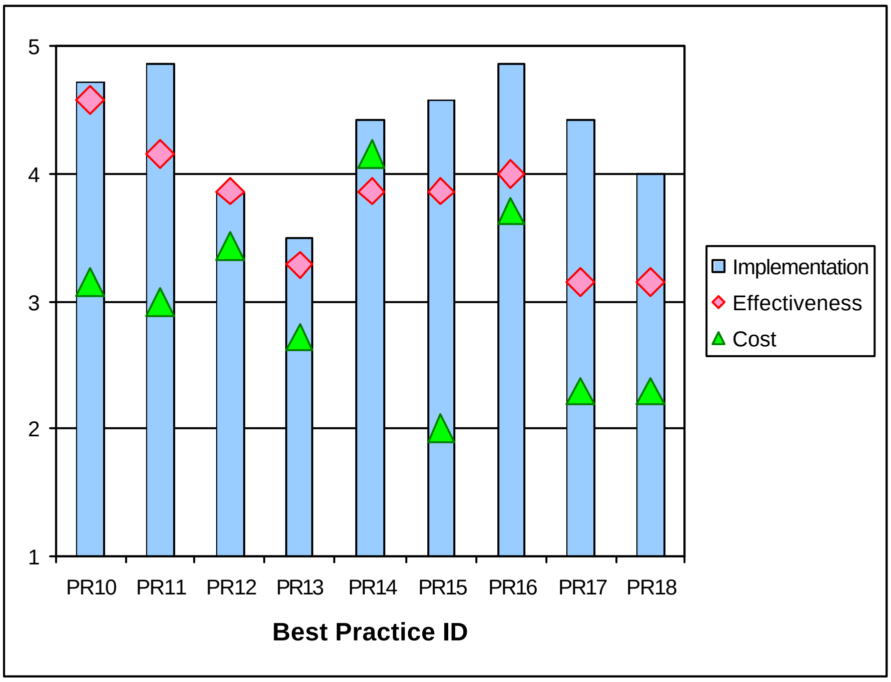


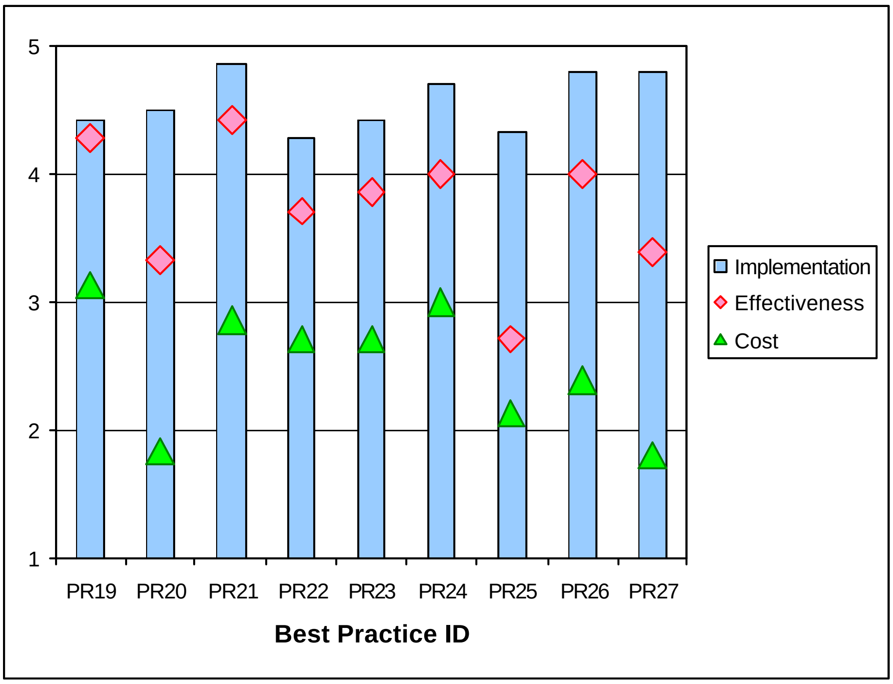
Appendix D –Service Provider Best Practice Questionnaire Results

The following three charts show the average rating of the Procedural Best Practices in terms of effectiveness, implementation, and cost (see the questionnaire in Appendix A for a description of these Best Practices). These Best Practices apply to Service Providers.



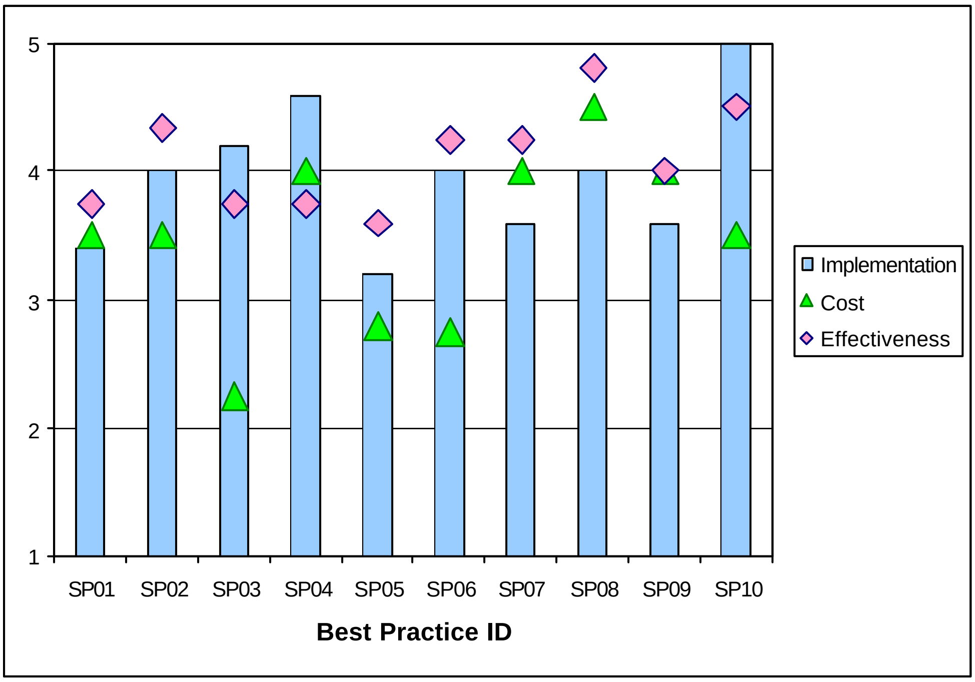
Appendix D –Service Provider Best Practice Questionnaire Results

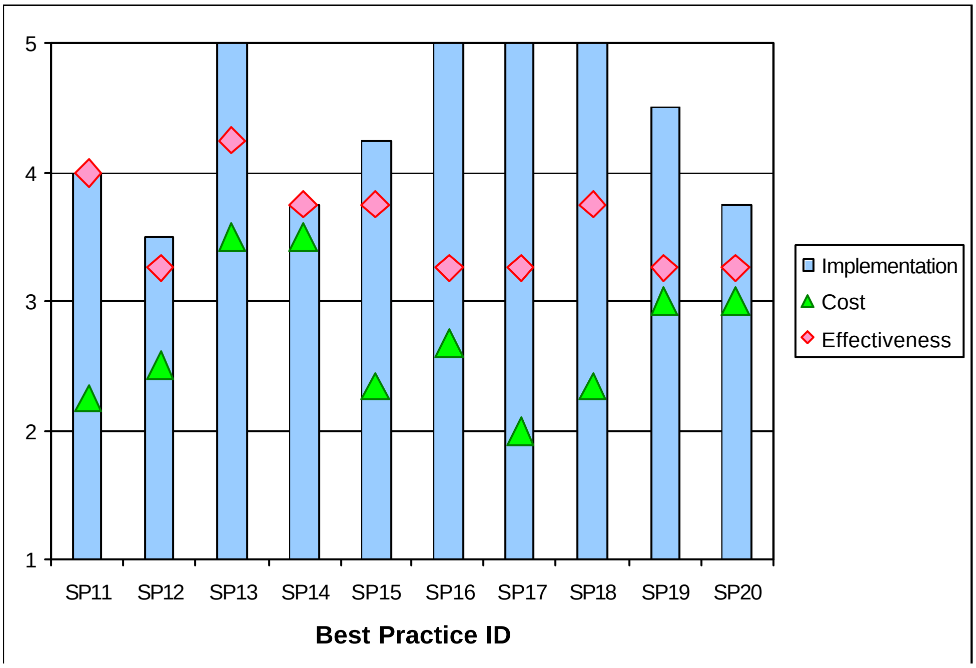


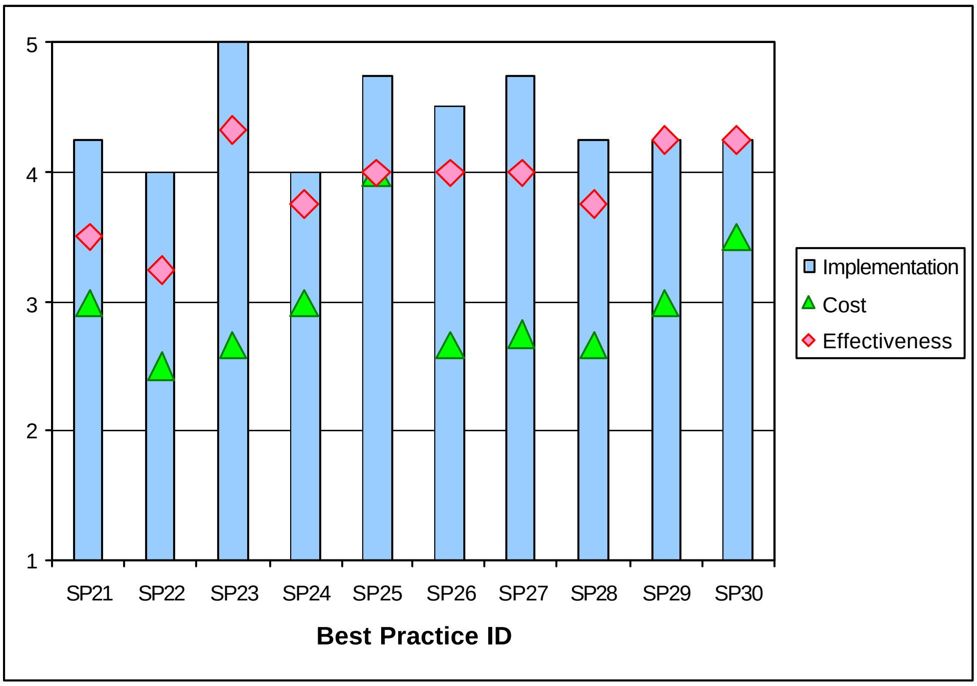


Appendix D –Service Provider Best Practice Questionnaire Results

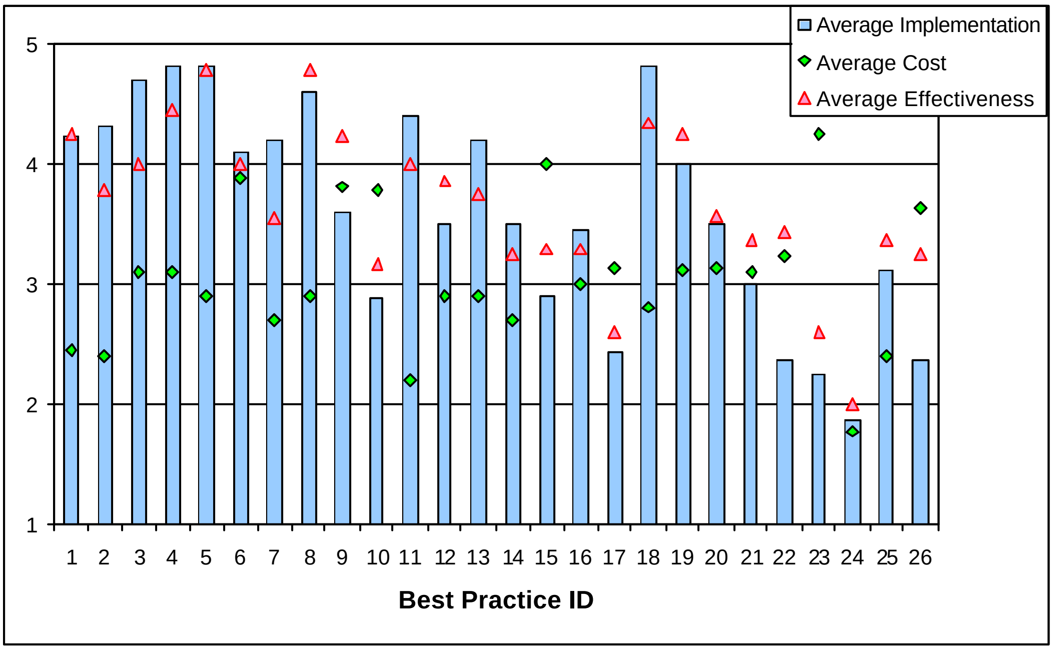
This Appendix provides three graphs which indicate how each of the “old” supplier Best Practices was rated on effectiveness, implementation, and cost. This Appendix provides results for the Supplier Best Practice Questionnaire that are listed in Appendix B. A high number for effectiveness indicates that the respondents believed that this Best Practice was highly effective in preventing outages. A high number for cost indicates that this Best Practice is very costly to implement (relative to other potential Best Practices). A high number for implementation indicates that this Best Practice is implemented everywhere.

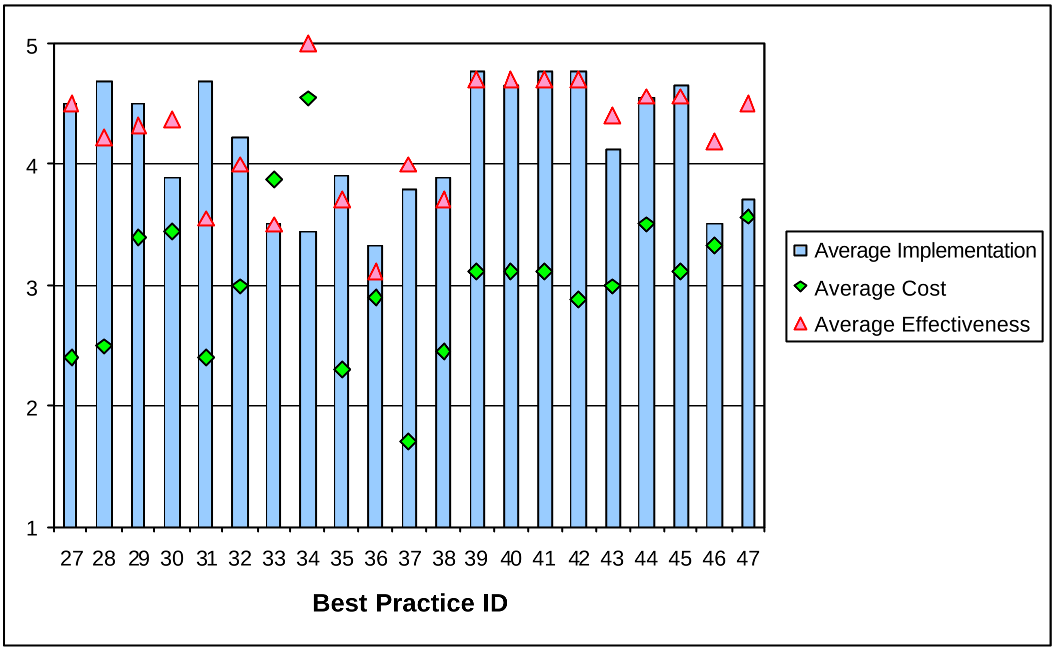


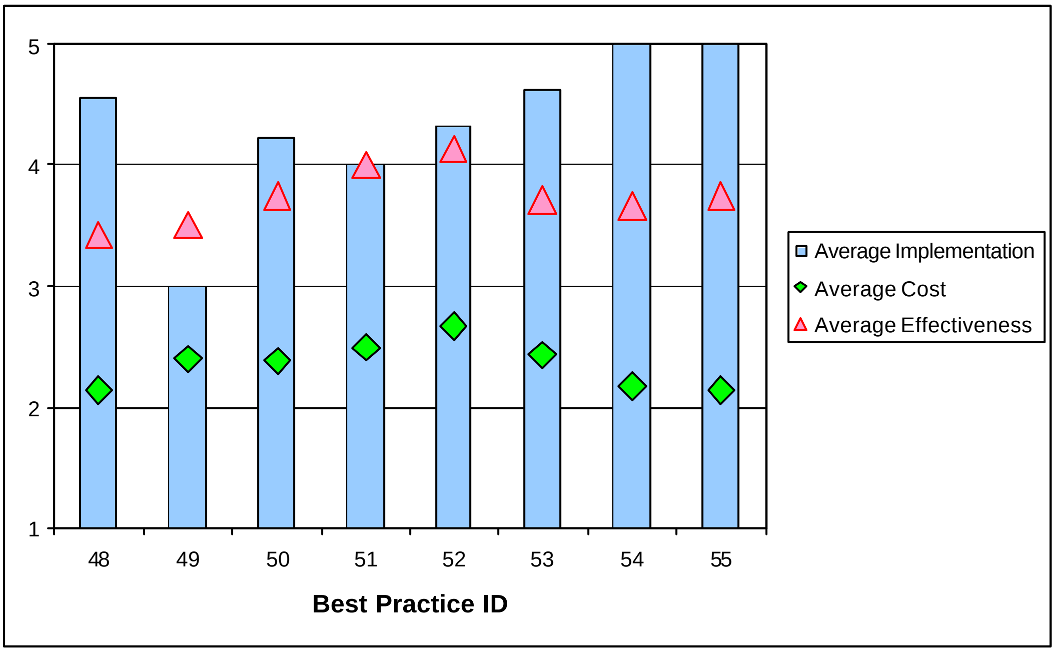



5
4
3
2
1
SP21
SP22
SP23
SP24
SP25
SP26
SP27
SP28
SP29
SP30
Best Practice ID
Implementation
Cost
Effectiveness

This Appendix provides three graphs which indicate how each of the "old" facilities Best Practices was rated on effectiveness, implementation, and cost. This Appendix provides results for the Facilities Best Practice Questionnaire that are listed in Appendix F. A high number for effectiveness indicates that the respondents believed that this Best Practice was highly effective in preventing outages. A high number for cost indicates that this Best Practice is very costly to implement (relative to other potential Best Practices). A high number for implementation indicates that this Best Practice is implemented everywhere.







5
4
3
2
1
48
49
50
51
52
53
54
55
Best Practice ID
Average Implementation
Average Cost
Average Effectiveness

Appendix F: NRIC IV Focus Group 3 Subcommittee 2 Report

Network Reliability Interoperability Council IV
Focus Group 3 Subcommittee 2

Data Analysis and Future Considerations Team
Report Index

Network Reliability Interoperability Council IV
Focus Group 3 Subcommittee 2

Data Analysis and Future Considerations Team

1. Executive Summary

Background

The current Federal Communications Commission (FCC) outage reporting requirements were developed following a series of major service outages in various local exchange and inter-exchange common carrier wireline telephone networks in the early 1990s. These outages were unprecedented in scale and scope, and raised concerns about the fundamental reliability of the nation’s public switched telephone network infrastructure. At the time, there were no objective measures available to allow an effective response. The FCC and the telecommunications industry worked together to codify the appropriate criteria and procedures for reporting major outages that became 47 CFR 63.100.

Today, the FCC outage reporting "process" has evolved into a cooperative one. The outage reports are available for use by other federal agencies and state public service commissions, which may reduce their need to request further reporting. Carriers gain insight into reliability issues from information sharing and identification of trends in outage causes and types. Customers benefit from the continuous focus on reliability improvement by service providers and equipment vendors.

Current Situation

Since the FCC first adopted its outage reporting rules in February 1992, the industry has changed dramatically. The FCC recognizes that the nation is interested in the reliability of communications services beyond the wireline switched voice services offered by telecommunications common carriers (which are subject to the outage reporting requirements). The wireline network represents a large but slowly growing segment of the telecommunications industry while other segments (CMRS [Commercial Mobile Radio Services], satellite, cable, data networking and Internet Service Providers [ISPs]) are expanding at rapid rates with new services. Some of these segments have now become significant portions of the overall telecommunications market. Periodically, service disruptions affecting "non-reporting" services such as satellite received widespread attention in the media.

The FCC has referred the matter to Network Reliability and Interoperability Council (NRIC IV) as reflected in the following section from the NRIC IV charter:

National Network Reliability: The committee will report on the reliability of public telecommunications network services in the United States and will determine whether "best practices" previously recommended should be modified or supplemented. It will also develop a proposal for future consideration relative to extending these best practices to other industry segments not presently included in current practices.

The FCC has never officially identified these "other segments". Neither has the FCC recommended reporting criteria for them. However, discussions with the Commission's staff have clarified this charge to include identifying additional industry segments, and recommending tools that the Commission may need to consider for inclusion in the reporting criteria for these additional segments. The industry segments that are of concern to the FCC are CMRS, satellite, cable, data networking and internet. Given the rapid increase in the public's reliance on these services, some collection of service disruption data may be appropriate to consider.

NRIC IV Focus Group 3 Subcommittee 2 has undertaken a review of current outage reporting processes for wire line carriers and made a suggestion for a direction for non-wireline service providers because:

- The public is increasingly dependent on services provided by non-wire line carriers.

- As a result, emerging segments have an increasing public safety impact.

Although the market penetration of non-wireline services is increasing, many consumers in business and residential markets employ a variety of wireline and no-wireline telecommunications services. The range extends from traditional circuit switched systems on the Public Switched Telephone Network (PSTN) to broadband systems based on frame relay and packet switching networks. The subcommittee recognizes that the range of service options now available may mitigate the impact of an outage in any one industry segment today. The committee also recognizes that there are interdependencies among these service options.

Recommendations

The Subcommittee developed a set of recommendations that were presented to NRIC IV on October 14, 1999. These recommendations are listed below and discussed in more detail in Section 5 of this report.

1. A voluntary trial is recommended with participation by service providers of CMRS (Commercial Mobile Radio Services), satellite, cable, data networking and Internet Service Providers (ISPs) to alert National Communications Systems/National Coordinating Center for Telecommunications (NCS/NCC) of outages that are likely to have significant public impact.

    - Industry associations should provide an informational notice to their membership to inform them of a voluntary outage reporting trial and encourage their participation.

    - Analysis of the data from the voluntary trial should be done by a neutral party. This analysis should be similar in scope to the analysis conducted on wireline carrier segments.

    - At the completion of a voluntary trial period (minimum 1-year) an evaluation of the effectiveness of the data for usefulness to participants and the FCC should be undertaken.

    - Data should be held confidential. A Freedom of Information Act (FOIA) exemption may be needed in order to facilitate participation in the voluntary trial.

    - A process for reporting data during the voluntary trial, including what report fields need to be populated and time frames for filing reports, has been addressed and is included in the Final Report.

2. Carriers should utilize the Network Reliability Steering Committee (NRSC) Wireline Outage Reporting Guidelines (Revised 1999) in compliance with Section 63.100. These guidelines reflect updated reporting requirements affecting 30,000 customer threshold, Fire related incidents, E911, and major airports list. The revised Guidelines also clarify who should report and under what conditions reporting is required.

3. A NRSC reporting template that provides a job aid for completing the FCC Service Disruption Reports should be utilized by industry segments currently reporting in compliance with 63.100. This template should also be used by industry segments that will report as part of the voluntary trial of outage reporting for CMRS, satellite, cable, data networking and Internet Service Providers. The template is available on the Alliance for Telecommunications Industry Solutions (ATIS) web site.

4. Industry communication of NRIC IV “Best Practices” to CMRS, satellite, cable, ISP, data networking service providers is recommended.

5. As technology continues to evolve and consumers increasingly have multiple paths for communication, reporting processes should be reviewed with an eye to eliminating redundant or non-value added reporting requirements.

Network Reliability Interoperability Council IV
Focus Group 3 Subcommittee 2

Data Analysis and Future Considerations Team

2. Background

The FCC initiated rulemaking to establish common carrier outage reporting requirements stating, "…we currently have no systematic way by which to become informed quickly of significant service outages, and we are unable to determine whether particular kinds of technology or equipment or other changes may threaten service reliability." These requirements addressed the Commission's need for real time notification of major outages in order to respond to inquiries, and to gather data upon which to base conclusions regarding the "health" of the nation's telecommunications infrastructure.

The initial Rules were adopted in February 1992 shortly before the FCC convened the original NRC and were based on the threshold for reporting on "customers". The Commission referred a number of issues with respect to outage reporting to the first NRC, now known as NRIC, which formed the Threshold Reporting Group (TRG) to address them. Subsequent rulemaking activities have further modified the requirements. Increased industry involvement has improved the ability of carriers to implement reporting and strengthened the relationship of the reporting requirements to service reliability and actual customer impact.

The NRSC was established by the NRC under the auspices of Alliance for Telecommunications Industry Solutions (ATIS). ATIS is an association open to all segments of the telecommunications industry. Telecommunications carriers, service providers and equipment manufacturers follow common standards and operating procedures to ensure interoperability between equipment and networks. The NRSC is a consensus based industry committee formed to, "analyze the industry's reporting of network outages to identify trends, distribute the results of its findings to industry, and where applicable refer matters to appropriate industry forums for further resolution, in order to help ensure a continued high level of network reliability."

The analysis performed by the NRSC provides a ready answer to the questions raised regarding the reliability of the nation's telecommunications infrastructure. This analysis also identifies areas where improvement efforts can most effectively be targeted. These areas are addressed by NRSC and NRC/NRIC efforts. These efforts have resulted in the development of a body of reliability improvement recommendations, or "best practices" that are being evaluated and revised by Subcommittee 1 of this Focus Group to assure they are viable and applicable to today's telecommunications networks. The "best practices" are currently being updated as part of NRIC IV and will be published on the ATIS web site in January, 2000.

2.1 Scope Statement

NRIC Focus Group 3 Subcommittee 2 developed a scope statement during its October and November 1998 meetings. It was refined throughout the team's work activities to reflect learnings acquired through the study and recommendation process. The scope statement listed below is the final iteration.

The scope of the NRIC IV Focus Group 3 Subcommittee 2 is to:

- ***analyze current outage reporting criteria and data with an emphasis on their effectiveness.***
- ***suggest clarification of the current reporting criteria for incidents on sub-network or leased capacity situations if appropriate.***
- ***identify additional industry segments (e.g., cable, Internet Service Provider, satellite, and wireless) and tools that the Commission may need to consider for inclusion in the reporting criteria.***
- ***assess the likely impact of new and changing technologies and services (e.g., internet services, ATM, Frame Relay) on network reliability.***
- ***review and consider similar efforts for outage reporting that are underway (e.g., CIAO Critical Infrastructure Assurance Office) for a singular outage reporting process, to multiple government and industry entities (e.g., FCC, Department of Commerce, NCS).***
- ***suggest a direction for reporting outages and/or incidents which adversely affect current and future telecommunications services.***

Figure 1: Scope Statement

2.2 Deliverables and Work Plan

Subcommittee 2 was chartered with their work initiative during the opening NRIC IV Meeting on October 14, 1998. Per the Work Plan (see below) Subcommittee 2 first met on November 3, 1998 and met regularly via conference calls and meetings. Its' recommendations were presented to the NRIC IV on October 14, 1999. Status reports were provided to the NRIC IV during their regular quarterly meetings and were available to the public via the NRIC IV web site.

Date/Time	*Logistics*	*Work Activity*
Oct. 14, 1998	*NRIC*	*Initial charter presented*
Nov. 3, 1998 *10:00 – 2:00*	*Meeting* *Newark Airport*	*Identify Team Members* *Draft Detailed Work Plan* *Review NRIC II Recommendations*
Nov. 24, 1998	*NRSC*	*Status Report on Subcommittee 2*
Dec. 8, 1998 *1:00 – 5:00*	*Meeting* *Atlanta*	*Draft Scope Statement* *Data Collection Discussion* *Presentation PDD 63*
Jan. 14, 1999	*NRIC*	*Status Report on Subcommittee2*
Jan. 21, 1999 *1:00 – 4:00*	*Conference Call*	*Finalize Scope Statement* *Identify Task Teams & Assign Members*
Feb. 24, 1999 *1:00 – 5:00*	*Meeting* *ATIS*	*Task Team Readouts & Discussion* *Finalize Work Plan Timeline*
Feb. 25, 1999	*NRSC*	*Status Report on Subcommittee 2*
Mar. 18, 1999 *1:00- 5:00*	*Meeting* *ATIS*	*Discuss Draft Questionnaire and Process* *Finalize Timeline, Funding Details, Survey Recipients*
Apr. 14, 1999	*NRIC*	*Readout*
Apr. 27, 1999 *1:00 – 4:00*	*Conference Call*	*Review Draft Recommendation Task Team 1* *Review Draft Outage Report Guidelines and Outage Reporting Template; Review Survey Status*
May 26, 1999 *1:00 – 5:00*	*Meeting* *ATIS*	*Status/Readout Task Teams* *Preliminary Review of Survey Results* *Presentation of "Alert Situation" Matrix*
May 27, 1999	*NRSC*	*Status Report on Subcommittee 2*
June 16, 1999 *10:00 – 3:00*	*Meeting* *Newark Airport*	*Task Team 1 Final Recommendations* *Report Template Feasibility Issues* *Review Survey Results* *Discussion "Alert Situations" Criteria*
July 1, 1999 *1:00 – 3:00*	*Conference Call*	*Review Surrogate Proposals for Industry Segments* *Review Survey Results* *Review NRIC 7/14 Presentation*
July 14, 1999	*NRIC*	*Subcommittee 2 Activities Status and Survey Results*
Aug. 6, 1999 *8:30 –1:30*	*Meeting* *ATIS*	*Review Final Survey Results* *Develop Industry "Alert Situation" Criteria*
Aug. 25, 1999 *1:00 – 5:00*	*Meeting* *ATIS*	*Discussion "Alert Situations"* *Review and gain consensus around final recommendations*
Aug. 26, 1999	*NRSC*	*Status Report on Subcommittee 2*
Oct. 7, 1999	*Meeting*	*Finalize "Alert Situation" Definitions*

1:00 – 5:00	*Newark Airport*	*Review Draft 1 of Final Report*
Oct. 14, 1999	*NRIC*	*Final Recommendations Readout*
Oct. 25, 1999 *1:00 – 4:00*	*Conference Call*	*Incorporate Feedback from NRIC into Final Report*
Nov. 22, 1999 *1:00 – 5:00*	*Meeting* *ATIS*	*Define details for Report distribution* *Wrap up open items*
Dec , 1999	*NRSC*	*Final Report Filed*
Jan. 6, 2000	*NRIC*	*Final Report Presentation*

Figure 2: Schedule/Work Plan

2.3 Organization of Technical Paper

Appendix J List of Figures

Network Reliability Interoperability Council IV
Focus Group 3 Subcommittee 2

Data Analysis and Future Considerations Team

3. Team Structure and Team Members

3.1 Subcommittee Membership

The Subcommittee is comprised of members representing businesses in the telecommunications and information industry. Representatives from competitive access providers, local exchange carriers, inter-exchange carriers, telecommunications equipment manufacturers, satellite, cable and key industry associations, including Internet Service Providers, were asked to participate in the subcommittee. The following list of people indicates the contributors to the Subcommittee effort.

Name	Company
PJ Aduskevicz*	AT&T
Ray Albers	Bell Atlantic
Brad Blanken	CTIA
Ayanna Caldwell	Ameritech
Rick Canaday	AT&T
Wayne Chiles	Bell Atlantic
Royce Davis	GTE Network Services
Perry Fergus	Booz Allen & Hamilton
Judy Glatz	AT&T
Glenn Grotefeld	Motorola
Rick Harrison	Telcordia Technologies
John Healy	Telcordia Technologies
Bill Klein	ATIS
J. R. Lofstedt	U S WEST
Norb Lucash	USTA
Gabor Luka	National Communications System
Spilios Makris	Telcordia Technologies
Clyde Miller	Nortel Networks
Clayton Mowry	SIA
David Opferman	Motorola
Gary Pellegrino	Bell Atlantic Mobile
Michael Posch	Ameritech
Karl Rauscher	Lucent Technologies
Ira Richer	Corporation for National Research Initiatives
Harold Salters	PCIA
Bill Scheffler	AT&T BIS
Andy Scott	NCTA
Scott Taylor	BellSouth

Jerry Usry	Sprint

* Team Leader

3.2 Task Team Members

The subcommittee organized into task teams to address key areas identified in the scope statement.

3.2a Interface Task Team

Task Team 1, the Interface Task Team reviewed ongoing efforts to gather data on outages (e.g., [CIAO] Critical Infrastructure Assurance Office) including criteria for a singular outage reporting process to multiple government and industry entities (e.g., Federal Communications Commission, Department of Commerce, National Communications System [NCS]). Team members were:

J. R. Lofstedt*
Gabor Luka
Perry Fergus

3.2b Current Process Task Team

Task Team 2, the Current Process Task Team analyzed current outage reporting criteria and data with an emphasis on its effectiveness and suggested clarification of the current reporting criteria for incidents on sub-network or leased capacity situations. Team members were:

Bill Klein*
Ayanna Caldwell
Rick Canaday
Wayne Chiles
Michael Posch
Jerry Usry

3.2c Future Considerations Task Team

Task Team 3, the Future Considerations Team identified additional industry segments and tools that the Commission may need to consider for inclusion in the reporting criteria and assessed a direction for reporting outages and/or incidents that adversely affect current and future telecommunications services. Team members were:

PJ Aduskevicz *
Rick Canaday
Glenn Grotefeld
Gary Pellegrino
Harold Salters
Ray Albers
Judy Glatz
Dave Opferman
Ira Richer

3.2d Recommendation Team

Task Team 4, the Recommendation Team suggested a direction for reporting outages or incidents that adversely affect current and future telecommunications services. The Recommendation Team developed the Subcommittee Final Report. Team Members were:

Judy Glatz*
Subcommittee Members

* Team Leader

Network Reliability Interoperability Council IV
Focus Group 3 Subcommittee 2

Data Analysis and Future Considerations Team

4. Data Collection and Analysis Methodology

4.1 Interface Task Team

To accomplish its work, the Interface Task Team began by reviewing current outage reporting criteria and information flows, and identifying activities and organizations that have a related role in the current FCC outage reporting process. As a part of this preliminary step, Presidential Decision Directive 63 (PDD 63) *Protecting America's Critical Infrastructure White Paper* was reviewed to identify entities which may have a role in future outage reporting processes and criteria development. PDD 63 outlines the administration's policy on critical infrastructure protection. The result of this initial activity was verification that specific organizations (i.e., National Communications System [NCS], National Infrastructure Protection Center [NIPC]), were expected to be the focus of continued data collection and analysis efforts. The role of another PDD 63 related organization, the Critical Infrastructure Assurance Office (CIAO), was also reviewed and found to have no operational outage reporting role. The CIAO is currently focusing on facilitating development of a national plan to ensure critical infrastructure protection.

The Interface Task Team then developed potential information sources and collected data on the organizations' objectives, activities, and plans related to outage reporting. Data was collected via a number of methods, including 1) reviewing mission statements, program plans, and concept of operations documents, 2) conversing with and interviewing organization representatives or support personnel via telephone or face-to-face, and 3) reviewing related information (e.g., organization Web pages, strategic planning documents).

Finally, the Interface Task Team synthesized the collected data, compared and contrasted organizational roles, responsibilities and plans, and developed recommendations for review by the other Subcommittee 2 Tasks Teams. The Interface Task Team generally worked as a team in its analysis efforts, with each member serving as a point of contact to a specific organization for data collection purposes. The team met and communicated throughout the study period in person, via e-mail and through telephone conference calls.

4.2 Current Process Team

4.2.1 Reporting Criteria

To accomplish its work, the Current Process Task Team began by reviewing the current outage reporting criteria with an emphasis on their effectiveness in meeting the Commission's goals to become informed quickly of serious disruptions, and to gather, analyze and share information useful to ensure network reliability.

Most outages are filed with the FCC pursuant to the Commission's Rules in Part 63.100 because they meet the primary reporting criteria: service to 30,000 or more customers being impacted for 30 minutes or more. The initial (primary) reporting criteria established by the Commission required the reporting of service disruptions impacting 50,000 or more customers for 30 minutes or more, but was amended on the recommendation of the Network Reliability Council. At that time, it was estimated that lowering the threshold would triple the number of central offices subject to reporting requirements, thereby providing significantly more reliability information to the Commission and industry, without overburdening either. The current threshold has achieved this balance. On average, over the first seven years of reporting, there have been 170 reportable outages annually which meet these criteria, providing more than enough data points for statistical analysis of these outages.

The FCC also established separate reporting requirements for outages affecting 911 Service. Based on the recommendation of the Threshold Reporting Group, during NRC I, carriers initially agreed to report service disruptions to E911 tandem switches, regardless of the number of lines affected, if the incident lasted for 30 minutes or more, without alternate routing being implemented. Subsequently in August 1994, the FCC ordered carriers to report outages "when more than 25% of the lines to any PSAP were disrupted and there was no automatic rerouting to an alternate PSAP". As a result of this more inclusive threshold, more than nine times the number of E911 service outages were reported under these requirements than had been reported previously, a far greater reporting burden than anticipated. Carriers sought reconsideration of these rules and the Commission subsequently revised the reporting requirements for E911 Service in its October 1995 Order. As a result, the reporting frequency reverted to previous levels. Most E911 outages reported also fall within the 30,000 customer/30 minute criteria discussed above. However, a small number fall below these criteria and for statistical reasons are analyzed separately by the NRSC. To date, the NRSC analyses of these outages as performed by the NRSC consistently track with the larger outages.

A third set of reporting criteria have been established for outages that occur due to fire. Under this requirement a carrier must report any fire-related incident that impacts 1,000 or more service lines for a period of 30 minutes or more. While the Commission was petitioned to exclude incidents where fires consume telephone poles and aerial cable, these petitions were denied. The Commission stated its interest in "network vulnerabilities even where the cause of an outage is beyond the control of a carrier ..." The frequency of fire-related outages is low and to date has not increased the reporting burden of carriers.

The final set of reporting requirements are those for "special facilities" such as major airports, major military installations, key government facilities, and nuclear power plants. Outages that meet the reporting criteria for major airports are submitted by the carrier directly to the FCC. "Mission affecting" outages at major military installations, key government facilities and nuclear power plants are reported first to the NCS. The NCS will then either forward it on to the FCC or hold the report at the NCS due to the critical nature of the outage. There have been a limited number of special facility outages reported to the Commission during the past six years, imposing little burden on reporting carriers. Analysis of these outages by the NRSC yields results similar to 911 outages that track consistent with larger outages.

4.2.2 Reporting Data

The Current Process Task Team also investigated the effectiveness of the data required in current outage reports. When submitting their final reports to the Commission, carriers are required to report the following information: the date and time of the commencement of the outage, the geographic area affected, the number of customers affected, the types of services affected, the duration of the outage, the number of blocked calls during the outage, the apparent or known cause of the outage, the name and type of equipment involved, the specific part of the network affected, methods used to restore service, steps taken to prevent recurrence of the outage, the root cause of the outage, and a listing and evaluation of any best practices or industry standards which may have eliminated or ameliorated outages of the reported type. Industry representatives, and particularly those on the NRSC Data Analysis Team, have indicated that these data are sufficient to analyze outages and recommend solutions. However, there is a lack of consistency among carriers in the quality of the data provided and the uniformity in how the data are reported to the FCC.

4.2.3 Sub-Network Leased Capacity

The Task Team also investigated the current criteria for incidents on sub-networks or leased capacity to determine if clarification of the criteria was necessary. The Task Team determined that the current definition for reporting these types of outages is sufficiently clear and complete. Carriers required to report outages pursuant to Part 63.100 must ensure that all appropriate field personnel responsible for outage reporting understand the reporting criteria.

4.3 Future Considerations Task Team

The Future Considerations Task Team determined that it needed information from segments of nontraditional telecommunications and information companies to fulfill its mission. These companies included CMRS, satellite, cable, data networking, and ISP companies. The Task Team developed a questionnaire to survey representatives of these industry segments on their practices for network monitoring, outage analysis and reporting, outage information sharing, customer notification, disaster recovery, mutual aid, and knowledge of earlier NRIC recommendations.

The remainder of this section describes the questionnaire and the process used to administer it. It also summarizes the number of responses from the various industry segments.

4.3.1 Questionnaire Description

The body of the questionnaire consisted of 16 questions, several of which had multiple subquestions. Most of the questionnaire was composed of checkboxes to lessen the effort required to fill it out.

Questions 1 and 2 were both aimed at information on network monitoring. Question 1 asked whether the company currently monitored the network for service degradation or service outage. Question 2 asked what parts of the network are monitored for service degradation or service outage. Major types of equipment in the inter-node network and in the access network were listed.

Question 3 asked for criteria used to define a service outage and service degradation. The question was open-ended. The last part of question 3 asked for the thresholds used to define various levels of service degradation and outage.

Question 4 addressed how service degradation or service outage is analyzed by the company. Subquestions asked whether the company analyzes the root cause of individual events, analyzes trends, prepares tracking reports, or maintains a historical file of reports.

Questions 5 through 7 were concerned with information sharing. Question 5 asked with whom any of this information was shared. Question 6 asked for a list of forums at which information is shared. Question 7 asked for any condition under which information sharing occurs.

Questions 8 and 9 were concerned with notification. In particular, Question 8 asked whether customers and government bodies were notified of service outage or degradation. Question 9 asked how customers were notified. Respondents were asked to check whether the mechanism was TV, radio, recorded announcement, etc.

Questions 10 asked whether the company had a disaster recovery plan.

Question 11 asked whether there were back-up facilities for services carried over leased facilities. The question was added because of recent outages over leased facilities.

Question 12 asked whether the company had formal or informal mutual aid agreements with other companies.

Questions 13 and 14 asked whether companies were familiar with NRC recommendations and whether they had implemented these recommendations.

Questions 15 and 16 were both about the impact measures. Question 15 asked whether the company was familiar with the T1A1.2 impact measure. Question 16 asked whether the company had implemented some other measure of customer impact.

A copy of the questionnaire is provided in Appendix A.

4.3.2 Data Collection and Analysis Process

Focus Group 3 Subcommittee 2 decided to use Telcordia Technologies as the central point for requesting, collecting, compiling and aggregating data for its teams. All data collected by Telcordia Technologies was treated as proprietary information. Specific references to individual respondents were removed and the Subcommittee only reviewed aggregated results.

The NRIC IV wanted a view of nontraditional segments of the industry. Subcommittee 2 contained representatives from PCIA, CTIA, NCTA, SIA, USTA, and ISPs. These representatives either provided names of contacts to whom the questionnaire was sent or directly sent the questionnaires to contacts. All questionnaires were returned via e-mail, fax or regular mail to Telcordia Technologies.

The original set of questionnaires was sent out on April 15, 1999. The original cutoff date for completing the questionnaires was May 1, 1999. This cutoff date was extended until July 9. By July 9, twenty-five questionnaires had been returned. The final total of completed questionnaires is listed in Figure 3 below. Several companies fit into more than one category. As a result, the numbers in the second column of Figure 3 reflect 31 segment responses from 25 companies.

The results were aggregated and summarized over all industry segments, and as the Subcommittee deemed appropriate by segment. Although the Subcommittee would have preferred a larger sample, the team believes that the results are indicative of companies in each of the industry segments. Telcordia Technologies forwarded graphs to the team that summarized the results to use as input for this report. In addition, open-ended responses to the questionnaire were sent to the team. The team then analyzed these graphs and tables. The team's conclusions appear in Section 5 of this report.

Industry Segment	No. of Segment Responses
Cellular/PCS/Other Wireless	13
ISP/Internet Operator	7
Satellite Services	4
Paging/Messaging	3
Cable Operator-Telephony	2
Network Wholesale Provider	1
SS7 Carrier	1
Total	31

Figure 3: Data Questionnaire Responses

Network Reliability Interoperability Council IV
Focus Group 3 Subcommittee 2

Data Analysis and Future Considerations Team

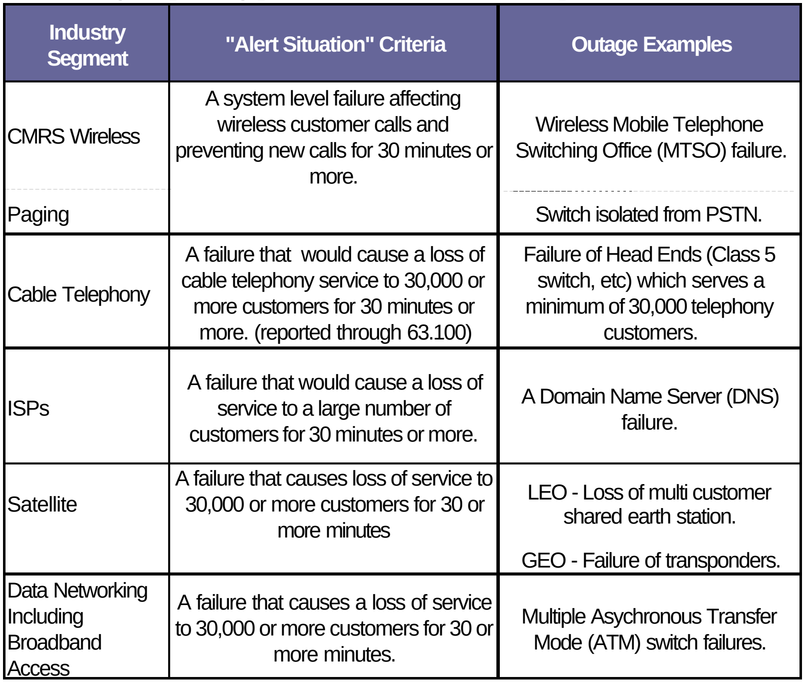
5. Findings and Recommendations

5.1 Interface Task Team Findings and Recommendations

The task team's initial investigation revealed that, aside from the current FCC outage reporting process, there exists no mandatory singular outage reporting criteria or process, and no data gathering or analysis, applicable to multiple government and industry entities. There are, however, several existing and proposed channels that providers of data and telecommunication services use to voluntarily share outage and intrusion information with public and/or private organizations, Government departments and agencies, and other entities. The figure below illustrates several of these channels as represented by the President's National Security Telecommunications Advisory Committee (NSTAC) in its report, *Telecommunications Outage and Intrusion Information Sharing Report*, June 1999. As stated earlier, the Interface Task Team focused its data collection efforts on two of these organizations, the NCS/NCC and the NIPC.

The limited scope was deemed appropriate because 1) both organizations are actively addressing future outage reporting process and criteria development, and 2) both have important roles in addressing PDD 63, which outlines the Administration's policy on critical infrastructure protection. NCC and NIPC-related findings are further discussed

Figure 4: Sample Information Sharing Channels



Industry Segment	"Alert Situation" Criteria	Outage Examples
CMRS Wireless	A system level failure affecting wireless customer calls and preventing new calls for 30 minutes or more.	Wireless Mobile Telephone Switching Office (MTSO) failure.
Paging		Switch isolated from PSTN.
Cable Telephony	A failure that would cause a loss of cable telephony service to 30,000 or more customers for 30 minutes or more. (reported through 63.100)	Failure of Head Ends (Class 5 switch, etc) which serves a minimum of 30,000 telephony customers.
ISPs	A failure that would cause a loss of service to a large number of customers for 30 minutes or more.	A Domain Name Server (DNS) failure.
Satellite	A failure that causes loss of service to 30,000 or more customers for 30 or more minutes	LEO - Loss of multi customer shared earth station. GEO - Failure of transponders.
Data Networking Including Broadband Access	A failure that causes a loss of service to 30,000 or more customers for 30 or more minutes.	Multiple Asychronous Transfer Mode (ATM) switch failures.

below. For specific information on the other organizations in the figure and their interrelationships, the reader is referred to the NSTAC report.

5.1.1 National Communications System (NCC)

The NCC was established in January 1984. As a joint industry-government operation, the NCC is the mechanism by which the federal government and the telecommunications industry jointly respond to national security and emergency preparedness (NS/EP) telecommunications service requirements. While the primary focus of the NCC is NS/EP telecommunications needs, the NCC also monitors the status of all essential telecommunications facilities including public switched networks.[1] Voluntary and cooperative outage reporting procedures are in place and support the NCC's efforts to promote the efficacy of NS/EP communications.

The NCC is operated by the Manager, NCS, and has participants representing telecommunications companies and Government departments and agencies. The NCC has two categories of participants, resident and nonresident. Resident industry participants are AT&T, COMSAT, GTE, ITT Industries, MCI WorldCom, National Telecommunications Alliance, and Sprint. Resident Government departments and agencies are the Department of Defense (DOD), Department of State (DOS), Federal Emergency Management Agency (FEMA), and General Services Administration (GSA). Non-NCC industry and government entities also may submit reports to the NCC.

As stated in the NSTAC report on outage and intrusion information sharing, reporting to the NCC is done using whatever means necessary to ensure the delivery of the information. Much of the reporting is done via public switched telephone network, e-mail, or in person through resident company or agency representatives. The use of encryption is being examined by the NCC and participating companies as a means of exchanging sensitive information.

The NCC is also responsible for reporting special facility outages to the FCC. Any mission-affecting telecommunications outage at any special facility (nuclear power plants, major military installations, and key government facilities) reported to the NCC that is expected to last or lasts at least 30 minutes is also reported to the FCC.

In addition to its traditional telecommunications-oriented role, the NCC is also developing a high-level concept of operations (CONOPS) for addressing enhanced cyber indications, assessment, and warning (IAW) capabilities. This effort aims to meet specific goals such as the ability to identify new or resurrected infrastructure intrusions and attacks, and to inform industry and facilitate implementation of mitigation strategies.

[1] Definitions of "NS/EP services" and "Essential" NS/EP can be found in FCC GEN Docket No. 87-505, NS/EP TSP System Report and Order, November 1988.

Currently, the NCC is engaged in requirement evaluation and program planning activities to support its recently-appointed Information Sharing and Analysis Center (ISAC) role. The ISAC is in the developmental stage with much discussion taking place. As conceptualized in PDD 63, the private sector will develop the design and function of an ISAC. It is envisioned that the ISAC will provide a mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC. The information sharing mechanism is not to interfere with any direct information exchanges between companies and the government. Potential ISAC information flow is illustrated in the figure below. Additional information on the ISAC can be found in PDD 63 and the previously referenced NSTAC report.

Figure 5: Potential ISAC Information Flow

The Interface Task Team believes that the NCC is well positioned to support ISAC capabilities. First, the NCC has a proven track record of supporting successful joint industry government information sharing. Mutual trust, vital to support information sharing, already exists between NCC government and industry representatives, and parties understand the sensitivities and implications of inappropriate disclosure of information. Additionally, the NCC has established information sharing policies and procedures that can be built upon to support required ISAC interfaces. The NCC is currently working with other entities (e.g., NIPC, CIAO) in conjunction with PDD 63 guidance.

5.1.2 National Infrastructure Protection Center (NIPC)

The Department of Justice and the FBI established the NIPC in February 1998 at FBI Headquarters in Washington, D.C. The mission of the NIPC is both a national security and law enforcement effort to detect, deter, assess, warn of, respond to, and investigate computer intrusions and unlawful acts both physical and "cyber," that threaten or target the nation's critical infrastructures. As envisioned in PDD 63, the NIPC serves as the national focal point for threat assessment, warning, investigation, and response to attacks on the critical infrastructures.

The NIPC is an interagency center operating within the FBI. As stated in the referenced NSTAC report, the center is designed to include representatives from the FBI, DOD, the intelligence community, other Federal departments and agencies, State and local law enforcement, and private industry.

As a relatively new organization, the NIPC is currently working to establish mechanisms to increase the sharing of vulnerability and threat information between the government and private industry, as well as with the NCC. Service providers from all industry segments should support development of information sharing channels between NCC and the NIPC to ensure the effectiveness of information sharing between the entities.

An example of NIPC information sharing is the InfraGard program which provides several functions for InfraGard members, including a forum for education and training on infrastructure vulnerabilities and protection measures, and the provision of threat advisories, alerts, and warnings. Types of information to be shared with the NIPC include actual or attempted computer intrusions involving critical infrastructures as well as physical attacks on the infrastructures. Private sector reporting of information to the NIPC is voluntary. Based on the above findings, the Interface Task Team made the suggestions listed below. Service Providers can also avail themselves of this reporting process.

- ♦ The NRIC should recognize the NCS/NCC as the focal point for joint government industry information sharing and support its developing ISAC mission. The existing FCC outage reporting process is complemented by current NCC processes and planned NCC capabilities (e.g., IAW capability, ICAS functions).
- ♦ To ensure the effectiveness of the NCC's developing ISAC role, all service providers should work cooperatively with the NCC to accomplish timely voluntary outage reporting objectives as they are developed. Additionally, to ensure that outage information is placed without delay into operational channels, the NCC's FCC standing representative, in care of the Manager, NCC, should be copied on all outage reports sent to FCC headquarters. Reports should be sent to:

FCC Standing Representative
Manager, NCS/NCC
701 South Courthouse Road
Arlington, Virginia 22204-2199

5.2 Current Process Task Team

The Task Team's investigation revealed that the current reporting criteria and data are sufficient and effective for use in analyzing outages and to develop recommendations to eliminate or mitigate the impact of similar outages in the future. However, there are concerns with the quality of the data reported and the uniformity of reporting by carriers. To this end, the Current Process Task Team makes the following suggestions:

1) All carriers required to report major network disruptions to the FCC should utilize the "Guidelines for FCC Reportable Outages" (Appendix D) to help identify situations that have the potential to be reportable to the FCC and to achieve greater industry uniformity in interpreting reporting criteria.

Focus Group 3 Subcommittee 2 Recommendation presented to NRIC IV 10/14/99

Carriers should utilize the Network Reliability Steering Committee (NRSC) Wireline Outage Reporting Guidelines (Revised 1999) in compliance with Section 63.100. These guidelines reflect updated reporting requirements affecting 30,000 customer threshold, Fire related incidents, E911 and major airports list. The revised Guidelines also clarify who should report and under what conditions reporting is required.

2) To assist the industry in gaining a better understanding of outages and their causes and to provide greater uniformity of reporting among carriers, all carriers are required to report major network disruptions to the FCC. Carriers should use the "Outage Reporting Template" (Appendix E) and "Instructions for Completing Outage Reporting Template" (Appendix F) for filing both their Initial and Final Service Disruption reports.

Focus Group 3 Subcommittee 2 Recommendation presented to NRIC IV 10/14/99

A NRSC reporting template that provides a job aid for completing FCC Service Disruption Reports should be utilized by industry segments currently reporting in compliance with 63.100. This template should also be used by industry segments that will report as part of the voluntary trial of outage reporting for CMRS, satellite, cable, ISP and data networking service providers. The template is available on the Alliance for Telecommunications Industry Solutions (ATIS) web site.

3) In order to further standardize the reporting methodology the NRSC may want to undertake a thorough examination of the direct cause and root cause definitions currently utilized for analysis of outages. This analysis would be for the purpose of further clarifying the definitions and developing additional "causes" and/or elimination of "causes".

4) In order to enhance the industry's ability for consistency in its reporting of outages, the NRSC should take the necessary steps to make the Outage Reporting Template electronically accessible via the Internet.

5.3 Future Considerations Task Team

5.3.1 Survey Results

Figure 6: Indicates that all respondents monitor service degradation/outages either locally, on a centralized basis or both.

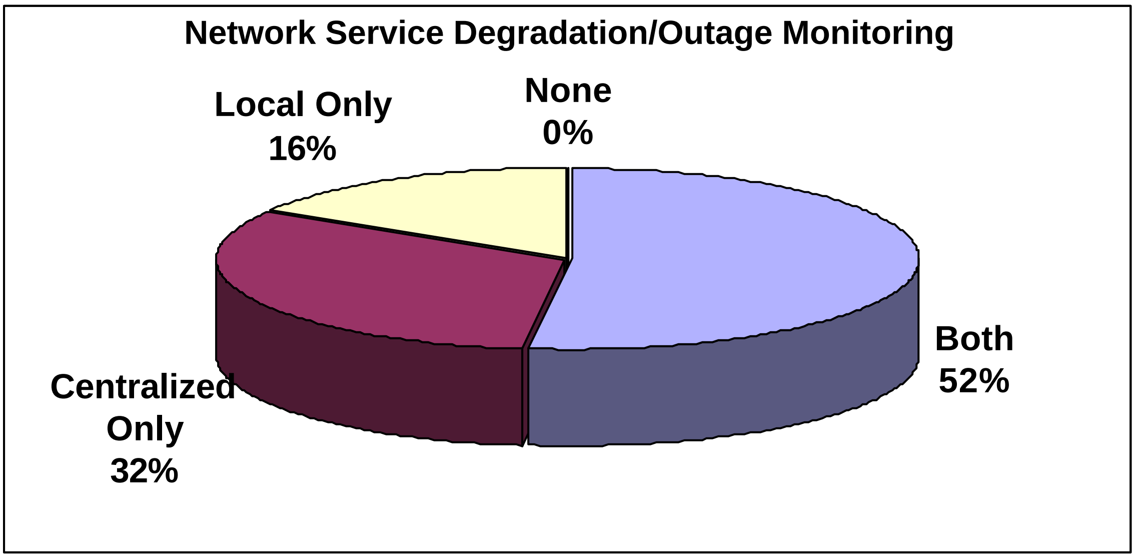
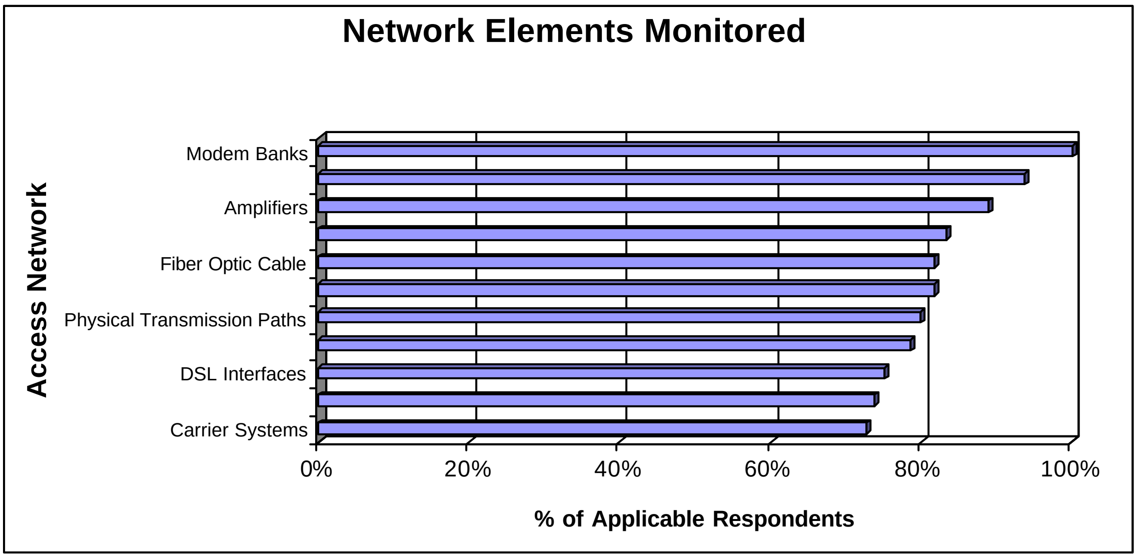


Figure7: Indicates Access Network Elements that are monitored by respective industry



segment.

Figure 8: Indicates additional network elements that are monitored by respective industry segment

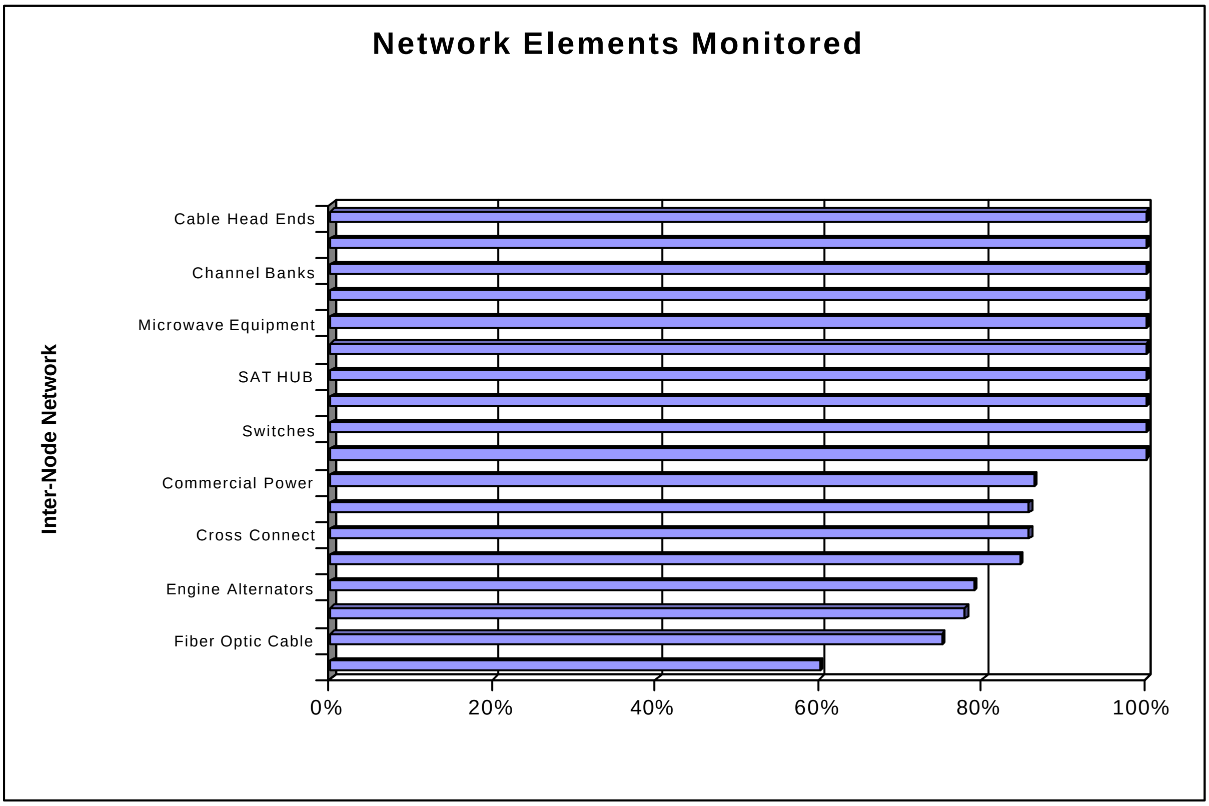


Figure 9: Displays the % of respondents who monitored for Equipment Failure, Power, Site Environmental, Overload, Fire, and Physical Access.

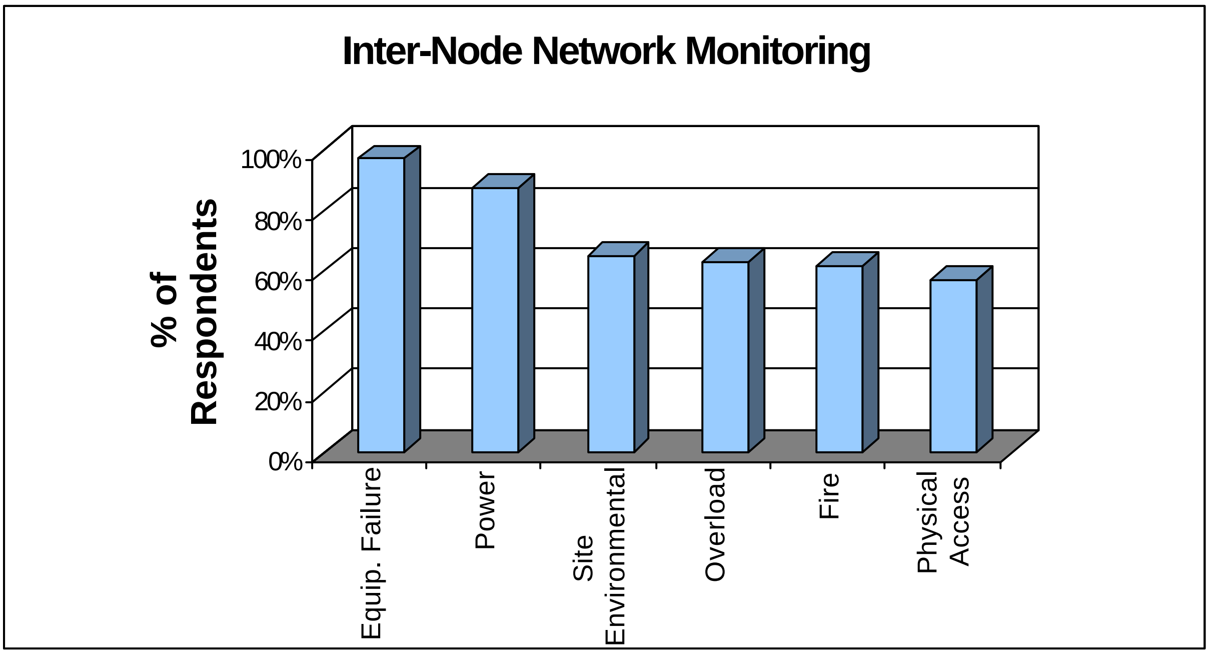


Figure 10: Shows that 72% of respondents have Disaster Recovery Plans in place.

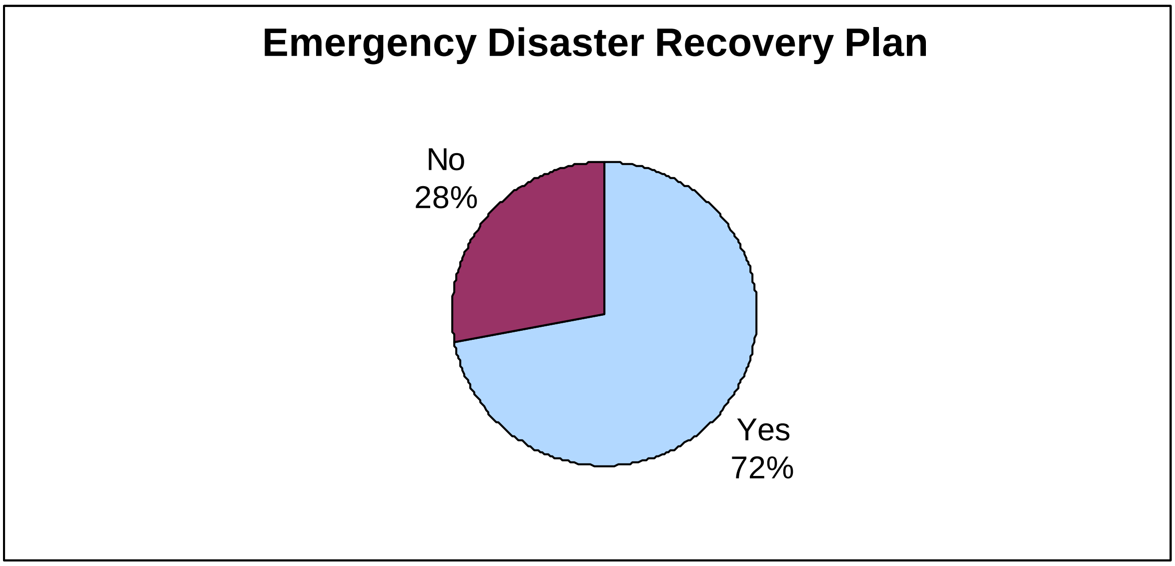


Figure 11: A Significant amount of root cause analysis was reported by respondents.

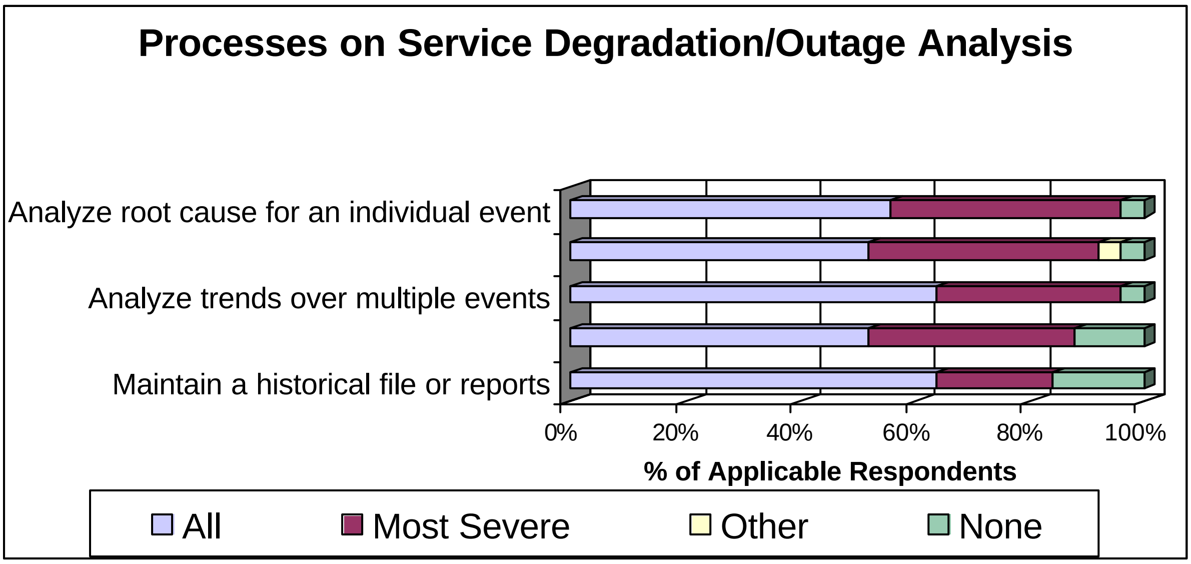


Figure 12: Displays the types of information sharing which occurs. Information on service degradation/outage is shared internally and with vendors. Less sharing is done with other companies and industry forums. This may be due to the strongly competitive market and/or relative immaturity of some industry segments.

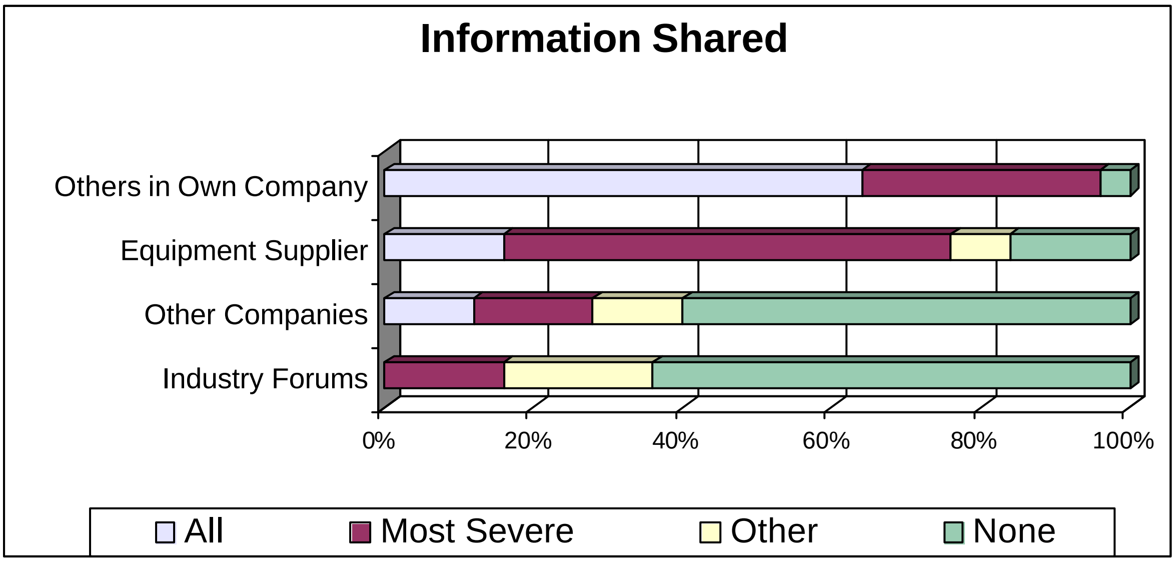


Figure 13: 82% of respondents notified customer of service degradation/outage.

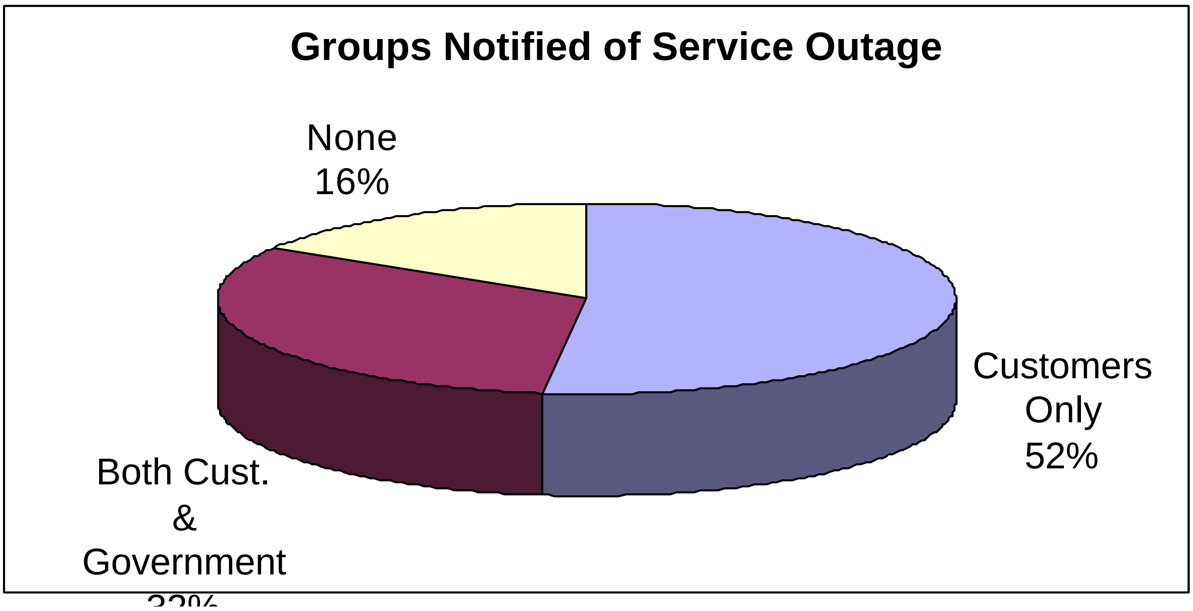
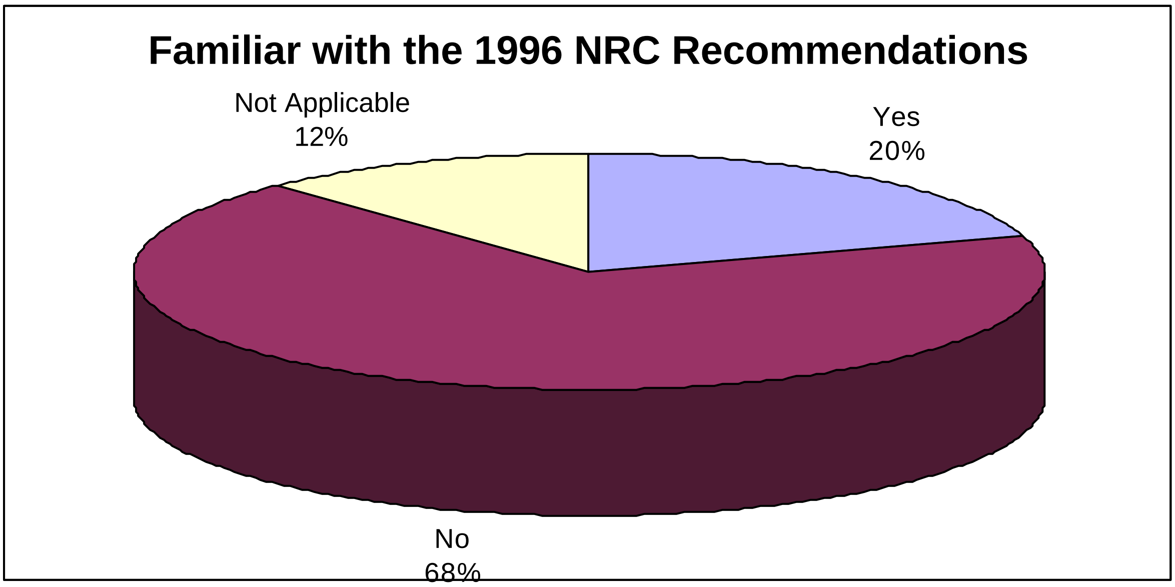


Figure14: Indicates an information sharing opportunity for non-wireline industry segments that are not familiar with NRC recommendation.



5.3.2 Proposed Voluntary Trial of Outage Reporting

As determined by previous NRIC reports, information sharing among service providers within an industry can promote an improvement of services provided to business users and consumers. For industries not currently reporting outages, information sharing within an industry and across industry segments may help identify common problems that may be best addressed by joint action.

Discussions were held with representatives (from service providers, manufacturers, and trade associations) of CMRS, satellite, cable, ISP and data networking service providers. Supported by subject matter experts in the current outage reporting methodology, a number of industry segment representatives identified the need for different methodologies for defining the extent of outages and their impact on the public. In those segments, neither “lines” nor “blocked calls” may be measurable quantities that accurately relate to “customers” affected by an outage.

Focus Group 3 Subcommittee 2 Recommendation presented to NRIC IV 10/14/99

A voluntary trial is recommended with participation by service providers of CMRS (Commercial Mobile Radio Services), satellite, cable, data networking and Internet Service Providers (ISPs) to alert NCS/NCC of outages that are likely to have significant public impact.

- **Industry associations should provide an informational notice to their membership to inform them of the voluntary outage reporting trial and encourage their participation.**
- **Analysis of the data from the voluntary trial should be done by a neutral party. This analysis should be similar in scope to the analysis conducted on wireline carrier segments.**
- **At the completion of the voluntary trial period (minimum 1-year) an evaluation of the effectiveness of the data for usefulness to participants and the FCC should be undertaken.**
- **Data should be held confidential. A Freedom of Information Act (FOIA) exemption may be needed in order to facilitate participation in the voluntary trial.**
- **A process for reporting data during the voluntary trial, including what report fields need to be populated and time frames for filing reports has been addressed and is included in this report.**

Industry Segment	"Alert Situation" Criteria	Outage Examples
CMRS Wireless	A system level failure affecting wireless customer calls and preventing new calls for 30 minutes or more.	Wireless Mobile Telephone Switching Office (MTSO) failure.
Paging		Switch isolated from PSTN.
Cable Telephony	A failure that would cause a loss of cable telephony service to 30,000 or more customers for 30 minutes or more. (reported through 63.100)	Failure of Head Ends (Class 5 switch, etc) which serves a minimum of 30,000 telephony customers.
ISPs	A failure that would cause a loss of service to a large number of customers for 30 minutes or more.	A Domain Name Server (DNS) failure.
Satellite	A failure that causes loss of service to 30,000 or more customers for 30 or more minutes	LEO - Loss of multi customer shared earth station. GEO - Failure of transponders.
Data Networking Including Broadband Access	A failure that causes a loss of service to 30,000 or more customers for 30 or more minutes.	Multiple Asychronous Transfer Mode (ATM) switch failures.

The table above was developed to suggest examples of outage indicators that might be used for reporting during the voluntary trial. The thresholds for reporting by industry segment may need to be adjusted during the voluntary trial period to strike a balance between too many reports that would result in undue reporting burden and too few reports that would provide insufficient data analysis.

This voluntary trial will be designed to balance consistency across industry segments with accurate representation of the impact of outages. Consistency will also extend to complementing current reporting required by 47 CFR 63.100.

To increase the synergy with reporting being developed to implement PDD 63, the reports for industry segments not currently reporting outages will be provided to the NCS/NCC in its role as an Information Sharing and Assessment Center.

5.3.3 Outage Reporting

The subcommittee recommends the use of an initial outage report and final outage report procedure for the voluntary trial, similar to Wireline Outage Reporting Process outlined in 47 CFR 63.100. The initial outage report should be filed within 24 hours of the outage in order to provide timely information to the NCS/NCC. This will allow NCS/NCC to identify potential multi-site and/or multi-operator outages that could be indicative of natural, accidental, or deliberate outages, some of which may then trigger further action under PDD 63. However, filing of the initial outage report should not impact the timeliness of restoring service.

The final outage report (within 30 days of the initial outage report) should provide comprehensive data on each outage. This data will allow in depth analysis of the outages similar to the way that the NRSC performs analysis for outage reported under 47 CFR 63.100. The matrix below shows the recommended mandatory and optional field to be provided for the initial and final report.

LIST I.D.	CFR 47 S 63.100 Ref. for Wireline	Field Description	Required Field
INITITAL REPORT			
I-a	(c)(d)	carrier/service provider	Required
I-b	(b)(c)(d)(e)(g)	contact person	Required
I-c	(b)(c)(d)(e)(g)	telephone number of contact person	Required
I-d	(b)(c)(d)(e)(g)	start date	Required
I-e	(b)(c)(d)(e)(g)	start time of impact (local, including time zone)	Required
I-f	(b)(c)(d)(e)(g)	geographic area affected (general)	Optional
I-g	(b)(c)(d)(e)(g)	estimated number of customers affected	Optional
I-j	(b)(c)(d)(e)(g)	apparent or known cause (high-level event description)	Optional

Figure 15: Initial Voluntary Trial Report Information Fields

The following field definitions are based on what is currently utilized by the NRSC in its analysis of outages.

- **Carrier/Service Provider**: provide the name of the carrier or service provider filing the outage report.
- **Contact Person**: provide the name of the individual reporting the outage. This should be the person who should be contacted to provide further information concerning the outage.
- **Telephone Number of Contact Person**: provide the telephone number at which the person above can be reached.
- **Start date**: provide the date when the outage started for the geographic area of the outage. For outages that may span multiple time zones and have separate dates in each time zone, select the date in the time zone estimated to be most affected. The location of the outage may be different from location of the person reporting the outage.
- **Start time of the impact (local, including time zone):** provide the time (local time at the location of the outage not the time at the reporting location) of the commencement of outage (24-hour clock). In most cases both the physical location

of the outage and the majority of customers affected by the outage are in the same time zone. However, some outages have wide-ranging impacts and at times the greatest customer impact may not be at the physical location of the outage. If this is the case, use the time zone of the geographic area most affected.

- **Geographic Area Affected (general):** provide the (primary) city and state impacted by the outage. For outages with wide-ranging impact, descriptions such as "Southwestern Texas" or "Northeastern United States" may be more appropriate and descriptive.
- **Estimated Number of Customers Affected:** provide the estimate at the time of the initial outage report of the number of customers affected by the outage event.
- **Apparent or Known Cause (high-level event description):** provide the best estimate at the time of the initial outage report as to the apparent or known cause(s) of the outage event. Examples: commercial power failure, fire, earthquake, cable cut, software error, hardware failure, etc.

LIST I.D.	CFR 47 S 63.100 Ref. for Wireline	Field Description	Required Field
FINAL REPORT			
F-a	(c)(d)	carrier/service provider	Required
F-b	(b)(c)(d)(e)(g)	contact person	Required
F-c	(b)(c)(d)(e)(g)	telephone number of contact person	Required
F-d	(b)(c)(d)(e)(g)	start date	Required
F-e	(b)(c)(d)(e)(g)	start time of impact (local, including time zone)	Required
F-f	(b)(c)(d)(e)(g)	geographic area affected (general)	Required
F-g	(b)(c)(d)(e)(g)	estimated number of customers affected	Required
F-h	(b)(c)(d)(e)(g)	types of services affected (if applicable)	Required
F-I	(b)(c)(d)(e)(g)	duration of outage	Required
F-j	(b)(c)(d)(e)(g)	apparent or known cause (high-level event description)	Required
F-k	(b)(c)(d)(e)(g)	name of equipment involved	Optional
F-l	(b)(c)(d)(e)(g)	type of equipment involved	Optional
F-m	(b)(c)(d)(e)(g)	specific part of network affected	Required
F-n	(b)(c)(d)(e)(g)	methods used to restore service	Optional
F-o	(b)(c)(d)(e)(g)	steps taken to prevent recurrences	Required
F-p	(b)(c)(d)(e)(g)	root cause & trouble found	Optional
F-q	(b)(c)(d)(e)(g)	applicable Best Practices	Optional

Figure 16: Final Voluntary Trial Report Information Fields

Final Report Information Fields are listed and described below. Because greater understanding of the outage event is likely as the final report is prepared, information fields may change between the initial report and final report.

- **Carrier/Service Provider**: provide the name of the carrier or service provider filing the outage report.
- **Contact Pers on**: provide the name of the individual reporting the outage. This should be the person who should be contacted to provide further information concerning the outage.
- **Telephone Number of Contact Person**: provide the telephone number at which the person above can be reached. A fax number and e-mail address would also be helpful.
- **Start date**: provide the date when the outage started for the geographic area of the outage. For outages that may span multiple time zones and have separate dates in each time zone, select the date in the time zone estimated to be most affected. The location of the outage may be different from the location of the person reporting the outage.
- **Start time of the impact (local, including time zone):** provide the time (local time at the location of the outage not the time at the reporting location) of the commencement of outage (24-hour clock). In most cases both the physical location of the outage and the majority of customers affected by the outage are in the same time zone. However, some outages have wide-ranging impacts and at times the greatest customer impact may not be at the physical location of the outage. If this is the case, use the time zone of the geographic area most affected.
- **Geographic Area Affected (general):** provide the (primary) city and state impacted by the outage. For outages with wide-ranging impact, descriptions such as "Southwestern Texas" or "Northeastern United States" may be more appropriate and descriptive.
- **Estimated Number of Customers Affected:** provide the estimate at the time of the final outage report of the number of customers affected by the outage event. Additional rules for identifying customers affected for the final report will be detailed in a separate document. Need to include details on document referenced.
- **Types of Services Affected (if applicable):** provide a short list of service(s) affected, if the service provider has key distinctions among different services offered. Among the key distinction to identify is access to 911 Service. Additional rules for identifying the types of service affected will be detailed in a separate document. Need to include details on document referenced.
- **Duration of Outage:** provide the duration from the time of the outage start until substantially all service is restored to the customers affected. Additional rules for identifying when "substantially all service is restored" shall be detailed in a separate document. Included will be rules governing how to identify restoration of some services to some customers during the period of the outage duration.
- Need to include details on document referenced.
- **Apparent or Known Cause (high-level event description):** provide the determined cause(s) of the outage based on analysis of the data collected surrounding the event. Examples: commercial power failure, fire, earthquake, cable cut, software error, hardware failure, etc.
- **Name of Equipment Involved:** provide the vendor name of the equipment involved in the outage.
- **Type of Equipment Involved:** provide the specific equipment (including release) involved in the outage.

- **Specific Part of Network Affected:** e.g., tandem switch, signaling network, central office power plant, outside plant cable, mobile switching center, etc.
- **Methods Used to Restore Service:** provide a chronological narrative of the methods used to restore service, both "quick fix" and final. For example, this description would include steps such as automatic system restoration, manual intervention activities performed to restore service, (e.g., replaced circuit pack, reboot software).
- **Steps Taken to Prevent Recurrence:** describe what steps have or will be taken by the carrier/service provider to implement, at both this location and throughout its network(s) if appropriate, the corrective actions identified through its Root Cause Analysis of this incident. If a time frame for implementation exists, it should be provided. If no further action is required or planned, the carrier should so indicate.
- **Root Cause and Trouble Found:** provide the direct and root causes of the event. The direct cause is the action or procedure that triggered the incident. The root cause is the key problem, which once identified and corrected prevents the same or a similar problem from recurring. It is not uncommon that two or more problems may be closely linked and may require detailed investigation. However, in any single incident there should be only one root cause. Appendix F provides a comprehensive list and description of direct and root cause categories currently used by the NRSC for Wire Line Outage Reporting.
- **Applicable Best Practices:** provide a listing and evaluation of the effectiveness in the immediate case of any "best practices" or industry standards identified by the Network Reliability Council (NRC) successor Network Reliability and Interoperability Council (NRIC) to eliminate or ameliorate outages of the reported type. Include any "best practices" that were not used and that may have eliminated the outage or ameliorated the effects of the outage. Recommendations of the NRC/NRIC may be found in:

  "Network Reliability: A Report to the Nation", June 1993
  "Network Reliability: The Path Forward", April 1996
  "Network Interoperability: The Key to Competition", July 1997
  "NRIC IV Focus Group 3 Subcommittee 1 Report" December, 1999

Focus Group 3 Subcommittee 2 Recommendation presented to NRIC IV 10/14/99

Industry communication of NRIC IV "Best Practices" to CMRS, satellite, cable, ISP and data networking service providers is recommended.

5.3.4 Industry Communication of Voluntary Trial

Industry communication to "non-traditional" telecommunications segments to improve awareness of the NRIC IV report and Part 63.100 requirements are outlined in this section.

Industry associations can provide the following informational material to "non-traditional" segments:

- A direct mailing informational notice with a summary of the voluntary outage reporting trial including the template.
- NRIC IV Focus Group 3 Subcommittee 2 Report, including a reference to the ATIS web page.
- Information on infrastructure equipment user groups who can provide expertise to "non-traditional" telecommunications segments.
- Informational notice with a summary of the voluntary outage reporting trial, including the template and a description of the implementation process.

5.3.5 "A New FCC for the 21st Century"

The Draft Strategic Plan for the New FCC for the 21st Century (released August 12, 1999) was reviewed during the latter stages of the activities of this subcommittee. This subcommittee has not thoroughly reviewed the plan, but has found a number of sections that imply that new approaches should be taken in the next millennium that may have significant impact on future industry activities. The goals and objectives of the Draft Strategic Plan include:

Create A Model Agency for the Digital Age

- Lead the way in the Information Age
- Reorganize to create an agency infrastructure conducive to convergence
- Create a faster, flatter, more functional agency
- Preserve and increase the wealth of knowledge and expertise of FCC staff

Promote Competition in All Communications Markets

- Eliminate barriers to entry in domestic markets
- Deregulate as competition develops
- Enforce the rules so the businesses compete fairly
- Promote competition in international communication markets

Promote Opportunities for All Americans to Benefit from the Communications Revolution

- Ensure access for all Americans to existing and future communications services
- Promote opportunities to expand direct participation in existing and future communications businesses
- Foster a consumer friendly marketplace

Manage The Electromagnetic Spectrum (The Nation's Airwaves) in the Public Interest

- Create more efficient spectrum markets
- Increase the amount of spectrum available for use, particularly for new services.

The draft Strategic Plan further expands on point number 2 above:

Deregulate As Competition Develops

"Eliminating outdated rules will play an important role in accelerating the transition to fully competitive markets. Consumers ultimately pay the cost of unnecessary regulation. Thus, one of our primary objectives must be to deregulate as competition develops, and to substitute market-based approaches for direct regulation. In addition, we must resist imposing legacy regulations on new technologies. Our goal should be to deregulate the old instead of regulating the new."

As technology continues to evolve, consumers will increasingly have multiple paths for communications. With technology convergence, telecommunications devices are handling a variety of telecom network inputs. For example, many paging units today have an internet address as well as a PSTN telephone number and can just as easily receive a paging transmission from a web-based packet switched network as from a location in the PSTN. Likewise, many two-way pagers can transmit acknowledgements and/or originate messages completely independent of the PSTN. Wireless handsets will increasingly be equipped to handle web-based applications and protocols.

In the context of recommending a voluntary trial, this committee urges a close review of reporting processes with an eye toward eliminating redundant or non-value added reporting elements. Mindful that a competitive telecommunications market is the best assurance of network reliability, this Subcommittee recommends the voluntary reporting results should be critically examined to assure that the information obtained is relevant in a rapidly changing and converging telecommunications environment.

Focus Group 3 Subcommittee 2 Recommendation presented to NRIC IV 10/14/99

As technology continues to evolve, consumers will increasingly have multiple paths for communications. This committee recommends continued review of reporting processes with an eye to eliminating redundant or non-value added reporting requirements. ***Check executive summary wording***

Network Reliability Interoperability Council IV
Focus Group 3 Subcommittee 2

Data Analysis and Future Considerations Team

6. Acknowledgements

Appendix G: NRIC IV Press Release – November 9, 1999

NETWORK RELIABILITY AND INTEROPERABILITY COUNCIL

For Immediate Release	**Contact: John Pasqua**
November 9, 1999	**Chairman, NRIC Steering Committee**
	908-542-6401; <jpasqua@att.com>

U.S. TELECOMMUNICATIONS INDUSTRY VIRTUALLY COMPLETES YEAR 2000 READINESS

Washington, D.C. – November 9, 1999, – The U.S. Telecommunications Industry is virtually complete with its Year 2000 remediation and implementation programs and local and long distance services are expecte d to continue to function on and after January 1, 2000.

In its latest, public report to the Federal Communications Commission (FCC), the Network Reliability and Interoperability Council (NRIC) IV announced that, based on input from telecommunications companies across the U.S., 100 percent of the switches, network elements and supporting software systems in the U.S. Public Switched Telephone Network (PSTN), owned by large, Local Exchange Carriers (LECs) and large, long distance Inter-Exchange Carriers (IXCs), have been made Y2K ready. While small- and mid-sized LECs trail their larger LEC counterparts in achieving Y2K readiness, the NRIC reported that most of these carriers should be compliant by the end of December 1999.

ASSESSMENT OF U.S. TELECOMMUNICATIONS INDUSTRY

The NRIC cited a recent FCC survey of 1,061 small- and mid-sized carriers, where 54 percent reported that they were Y2K ready at the end of June. The report went on to say that by the end of September, 92 percent of these carriers projected they would be Y2K ready and more than 98 percent expected to be Y2K ready by the end of December. Other surveys, independent of the FCC, conducted by the National Telephone Cooperative Association (NTCA) and the U.S. Department of Agriculture/Rural Utility States (USDA/RUS) have also projected more than 98 percent Y2K readiness of these small- and mid-sized carriers by December 1999.

The NRIC also reported that call processing should not be affected by the century-date change based on extensive industry testing that has been accomplished. According to the NRIC report, no significant interoperability testing gaps were identified in Access and Inter-Exchange switches and signaling vendors. In addition, the NRIC report stated that interoperability testing by major LECs and IXCs had either been completed or was nearing completion and, in the process, no Y2K date-

change related anomalies had been encountered. Additional interoperability testing between a major IXC and an Enhanced Service Provider, e.g., SS7 provider for small/mid-sized companies, is in progress.

The NRIC reported that the risk of failure of the domestic PSTN, due to Y2K, is minimal. The report did point out, however, that an estimated two million access lines, which equates to less than one percent of the U.S. total access lines, served by small and mid-sized carriers, could be at risk, resulting in some service quality degradation over time. The FCC is developing a plan to assist these companies achieve Y2K readiness.

ASSESSMENT OF NETWORK RELIABILITY

The NRIC, with input from the Alliance for Telecommunications Industry Solutions' (ATIS) Network Reliability Steering Committee (NRSC), reported that there were 47 outage incidents in the past quarter across the telecommunications network. The report stated most failure categories were within control limits but that outage exceptions were found in power, digital cross connect systems and those for which the root cause was procedural errors. The NRIC report pointed out that the industry is addressing these exceptions through recently published NRSC Procedural Errors recommendations (www.atis.org) and through "Power" best practices from NRIC's Focus Group 3's Best Practices subcommittee. This subcommittee is also reviewing, modifying and supplementing the entire inventory of Best Practices to make them broadly applicable to all segments of the telecommunications and information industry.

In addition, the NRIC's Data Analysis and Future Considerations subcommittee developed guidelines and templates designed to remove ambiguities and improve the quality of telecommunications outage reporting. The NRIC also recommended a voluntary trial of at least one year, coordinated and conducted by the National Coordinating Center for Telecommunications of the National Communications System (NCC/NCS), to develop guidelines for the reporting of outages or incidents affecting telecommunications and information services that are currently not required to report outages.

ASSESSMENT OF INTERNATIONAL TELECOMMUNICATIONS NETWORKS

Based on input from various public and private assessments over the past quarter, the NRIC reported the risk profile of international traffic to and from the United States on and after January 1, 2000 has continued to improve. With 90 percent of U.S. international traffic or a total of 29B Minutes of International Telecom Traffic (MITT), to and from 53 countries, only 16 percent of that traffic remains at high risk of some problems on or after January 1, 2000. Since NRIC's July report, 21 percent of this international traffic has moved from high and medium risk to the low risk category resulting in a current total of 72 percent of this international calling being reported as low risk. The remaining 10 percent of the

U.S. international traffic or 3B MITT is to and from 171 other countries. Seventy percent of the traffic, however, is still in high risk.

The NRIC reported that additional testing had been completed under the auspices of the International Telecommunications Union (ITU) and ATIS, focused on major international gateway switch vendor equipment and North American service providers. No Y2K anomalies were found.

The risk of international call failure between North America and other world regions was also reported as being minimal. Potential impacts, however, of Y2K to international calling include:

- **Call set-up delay due to network congestion in some foreign networks;**
- **Degradation of service quality over time due to non-compliant components of some foreign networks.**

The NRIC also reported that unpredictable infrastructure failures in other utility industries worldwide had the potential to adversely impact telecommunications networks both domestically and around the world.

ASSESSMENT OF NETWORK ACCESS

The NRIC report also provided insight on the readiness of customer premises equipment (CPE) and systems that interface with the Public Switched Telecommunications Network (PSTN). The NRIC reported that that are no major problems or industry-wide issues that cannot be handled with planning, including emergency 911 call processing. The NRIC recommended that CPE suppliers and service providers share the following information with customers, suppliers and distributors:

- **Communicate current Y2K status of products;**
- **Communicate availability of Y2K upgrades;**
- **Make Y2K solutions available when needed;**
- **Share testing strategy/results;**
- **Share contingency plans with both customers and supply chain;**
- **Encourage distributors to reach end users;**
- **Share Y2K impact on non-compliant, legacy equipment.**

The NRIC report went on to point out that end users must:

- **Become informed about the CPE being used;**
- **Inventory all systems;**
- **Contact vendors to establish compliance status;**
- **Plan/budget for needed upgrades;**
- **Follow supplier recommendations;**
- **Develop a contingency plan;**

- **Validate that your major vendors have such a plan;**
- **Have emergency phone numbers ready in the event of a CPE problem.**

The NRIC also reported continuing improvement in the Y2K readiness of Public Safety Answering Positions (PSAPs), which are utilized by local governments in responding to 911 calls.

In a survey, conducted by the National Emergency Number Association (NENA) for the NRIC, it was determined that there is a total population of 4,300 PSAPs nationwide. The survey also determined that 99.7 percent of the 2,754 PSAPs, that responded to the NENA survey, would be Y2K ready by January 1, 2000. NENA will attempt to complete its vendor survey with non-respondents during the fourth quarter in an ongoing notification campaign with PSAP vendors on the need for Y2K readiness.

ASSESSMENT OF INDUSTRY-WIDE CONTINGENCY PLANNING

In its report, the NRIC also reviewed contingency planning efforts across the telecommunications industry. The NCC/NCS will act as the focal point for data collection (both from domestic and foreign sources) and notification, using the NCC's Y2K database. Participants in this contingency planning initiative include major LECs, IXCs, Industry Forums, ITU members and government agencies. When available, the NCC will share information with the FCC and the Information Coordination Center (ICC). At present, small and medium sized carriers do not have a viable approach for participation in this contingency planning program and the U.S. Telecommunications Association (USTA) is exploring the possibility of posting information on its web site for these carriers.

In conclusion, the NRIC reported that the U.S. telecommunications industry has taken and continues to take appropriate actions to achieve Y2K readiness in advance of the century-change date and that the public switched telephone network will continue to reliably function, interoperate and interconnect on and after January 1, 2000. Information regarding individual NRIC Focus Group presentations will be posted on the NRIC web site (http://www.nric.org). Information regarding other NRIC activities associated with general network reliability can be found at http://www.atis.org/atis/nrsc/nrscinfo.htm**.**

###

Appendix H: NRIC V Post-Year 2000 Survey Cover Letter

A. John Pasqua
ANS Program Management, Planning & Quality
Vice President
AT&T Network Services

Room 4DC107
900 Route 202/206N PO Box 752
Bedminster, NJ 07921-0000
908-234-3400
Fax 908 234-4002
pasqua@att.com

07 July 2000

To Members of NRIC V,

As we end the mid-year point of the first year of the new millennium, we also need to complete the analysis of the impact the date change may have had on our individual networks. We have developed the attached brief questionnaire to gather data across the industry. Please take a few moments to complete the form and return it by 21 July 2000 to:

Susan Aira
AT&T Network Services
Room 290A-14 Annex Building
290 Davidson Avenue
Somerset, NJ 08873

If you wish to complete the questionnaire electronically, you will find it on the NRIC Web site at http://www.nric.org/. Please e-mail the completed form to:

aira@ems.att.com

Your responses will be totally confidential. The results of this survey will be consolidated and presented at the 23 August session of NRIC V.

Thank you in advance for your participation. Please feel free to call me if you have any issues, questions, or concerns.

A. John Pasqua
NRIC V Focus Group 1

Appendix I: NRIC V Post-Year 2000 Survey

NETWORK RELIABILITY AND INTEROPERABILITY COUNCIL

POST YEAR 2000 DATA GATHERING

1. How many Y2K-related incidents did your company experience? ______________
2. What was the duration of the incidents? ______________

   Average duration? ______________

   Range? ______________

3. How many were *domestic* ______________

   versus *international*? ______________

4. How many of the incidents were *customer-affecting*? ______________
5. What business *processes* (e.g., provisioning, ordering, billing, etc.) were affected?

6. Have you incorporated Y2K *regression testing* into your current processes (YES/NO)? ● Yes ○ No

   - If yes, has this caused you any delays in delivering your products/services (YES/NO)? ○ Yes ● No

7. What is your company doing to follow up on Y2K-related *temporary fixes* (e.g., windowing)?

8. What *other approaches* have you taken to ensure that Y2K-related fixes are not compromised?

9. What is the *most valuable lesson learned* from the Y2K program that could be applied to other projects or programs?

10. What *other benefits* have resulted to your company from the Y2K program (e.g., updated inventories, accelerated retirements of applications, etc.)?

If you are aware of any reports in your industry/segment that may capture overall results on Y2K-related impacts, please list them below:

Thank you for completing this questionnaire!