TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

The Telecommunications Act of 1996,[1] enacted in February of 1996, fundamentally revised the Communications Act of 1934, and thereby changed telecommunications regulation in the United States. Included among the many changes was the addition of new Section 256, titled "Coordination for Interconnection."[2]

The general purposes of the Act are to foster innovation, competition and deregulation in telecommunications. Section 256 requires the Federal Communications Commission (FCC) to establish procedures to oversee coordinated network planning by telecommunications carriers and other providers of telecommunications service and permits the FCC to participate in the development of public network interconnectivity standards by appropriate industry standards-setting bodies. The purposes of Section 256 as stated in the statute are (1) to promote nondiscriminatory accessibility by the broadest number of users and vendors of communications products and services to public telecommunications networks, and (2) to ensure the ability of users and information providers to "seamlessly and transparently transmit and receive information between and across telecommunications networks."

In April of 1996 the FCC revised the charter[3] of its Federal Advisory Committee, the Network Reliability Council, to advise the FCC on how it might best accomplish the responsibilities placed on it by Section 256. To reflect this mission, the Commission changed the name of the Council to "The Network Reliability and Interoperability Council."

The Council was first organized by the FCC in 1992 to provide expert advice to the Commission on issues requiring technical expertise in telecommunications issues. Consistent with the requirements of the Federal Advisory Committee Act, the membership of the Council is broadly balanced to reflect the interests being addressed by its charter. It includes senior representatives from large and small local exchange telecommunications carriers, including both incumbent and competitive carriers; large and small interexchange carriers; terrestrial wireless and satellite service providers; cable television service providers; equipment manufacturers, of both network and customer premises equipment, representatives of institutional and residential consumers of telecommunications services; state regulators, telecommunications standards-setting bodies, various telecommunications related trade associations, and others.[4]

To develop the recommendations sought by the FCC, the Council met on a quarterly basis for one year. It organized several focus groups to study the issues raised by Section 256 and to

[1]Pub. L. No. 104-104, codified at 47 U.S.C. Sec. 151 et seq.

[2]Section 256 is reprinted herein at Appendix A.

[3]The revised Charter of the NRIC is attached as Appendix D.

[4] The organizations participating in the NRIC are listed in Appendix F.

develop recommendations for consideration by it. The Council made extensive use of electronic resources in accomplishing its work, including the use of home pages provided by the FCC (http:www.fcc.gov/oet/nric) and Committee T-1 (http:www.t1.org/index/4202.htm).

It posted drafts of the work developed by the focus groups at these locations as well as minutes of its quarterly meetings.

The attached Report reflects the contributions of more than 200 persons with technical expertise and background who participated in the Council's work, and is a general consensus of those contributors. The key messages of the Report are that:

- The objectives of Section 256 -- accessibility, transparency and seamless interoperability -- must be pursued in context with the other objectives of the Act, including fostering innovation, competition and deregulation in telecommunications;

- Competitive market forces, voluntary standards processes and agreements among service providers, equipment suppliers, and other participants, should be relied on as the primary vehicles by which to balance the various objectives;

- Various kinds of telecommunications equipment and various telecommunications services are not interoperable today, and are not expected to be so by consumers;

- The historical experience in telecommunications has been that consumer demand generally, but not always, will produce the best balance of innovation and interoperability;

- The voluntary, open, consensus-based standards-setting process as used in the U.S. has proven to be an effective way of striking the balance in telecommunications;

- That process can be improved in various ways (suggested improvements include improving access to the process by communities identified as being of concern in Section 256, particularly individuals with disabilities and customers in rural areas);

- The FCC and standards organizations should define liaison responsibilities to communicate more effectively on Section 256 issues;

- Standards alone cannot assure interoperability; bilateral agreements and interoperability testing are crucial to maintaining interoperability;

- Where voluntary action is not meeting a compelling national need for interoperability in a timely fashion, the FCC should mandate it;

- The FCC should develop a short list of nationally accepted services and require that no telecommunications service provider make any system-wide changes in or extensions to such services that would cause a subscriber to lose such services unless those changes or

extensions (1) are the product of the National Planning Process discussed in Section 4 of the Report and (2) provide an opportunity to the customer to maintain uninterrupted service;

- Risks to interoperability that might be caused by increased diversity of service providers can be minimized by templates that identify issues to be resolved in bilateral negotiations among service providers;

- The goals of competition and interoperability can be served by using electronic web pages to identify resources;

- Gateway interfaces that provide access to operating systems, fully-funded interoperability testing, and observation of established security guidelines and agreements promote competition while minimizing risks to interoperability;

- Concerns of congestion of the public switched network caused by Internet usage can be minimized by the use of a template that identifies issues to be resolved in bilateral negotiations among Internet service providers and telecommunications service providers.

- The reliability of the nation's wireline telecommunications network remains at the same general level reported by prior NRC studies. The single greatest risk to those networks continues to be damage to transmission facilities, and the most effective way of dealing with those risks continues to be the enactment of effective one-call legislation.

2. BACKGROUND

The Network Reliability Council was first organized by the FCC in January of 1992 following a series of major service outages in various local exchange and interexchange wireline telephone networks. These outages were unprecedented in scale and scope, and caused some of the public, the press, and the Congress to question the fundamental reliability of the nation's public switched telephone network infrastructure. The Council was organized as a Federal Advisory Committee under the provisions of the Federal Advisory Committee Act.[5]

The Council was composed of senior technical experts from all parts of the telecommunications service provider and service user communities. It was asked to review the causes of service outages, and to develop recommendations to reduce their number and their effects on consumers. The Council developed a 1,000 page report entitled "Network Reliability: A Report to the Nation." The report studied nine areas of interest, and developed recommendations in each area. It concluded that although public wireline networks have an average availability above 99.9%,[6] steps could and should be taken to improve even that level. The recommendations of the Council for changes in the Commission's service outage reporting rules were incorporated into Section 63.100.[7] The recommendations of the Council for the establishment of a cross-industry group of experts to monitor and analyze outage data and to share that analysis with the telecommunications industry resulted in the creation of the Network Reliability Steering Committee under the auspices of the Alliance for Telecommunications Industry Solutions (ATIS).

The Council was rechartered by the Commission in 1994 to provide its expert advice on whether it foresaw any developments that could threaten telecommunications network reliability in the future. It was asked to continue to evaluate network performance, but also to assess reliability concerns arising out of increased interconnections to the public switched network and new technologies being deployed within it. It was asked to provide guidelines for improving access to telecommunications services for emergency services and to evaluate regional impacts of service outages.

The Council's report – “Network Reliability: The Path Forward” -- was published in February of 1996 and is available electronically at: http://www.fcc.gov/oet/nrc. The five chapters of the report discuss network reliability performance, increased interconnection, changing technologies, essential communications during emergencies, and telecommuting.

---

[5]That act generally provides that when the federal government seeks consensus advice from those it regulates it needs to do so through the Federal Advisory Committee process.

[6]Report to the Nation, "Software and Switching System Reliability," at p.1.

[7]47 C.F.R. Sec. 63.100.

In discussing network interconnection, the report explained that maintaining reliability and interconnectivity of networks depends primarily on industry standards setting processes to establish "base standards" that constitute the minimum set of requirements that define interoperability. These standards are voluntary, with enforcement provisions largely left to agreements among service and equipment providers.[8] The consensus of the report was that newer technologies seeking to interconnect with the existing wireline network are expected to configure their networks to comport with wireline architectures and interfaces. New service providers and developers of new technologies were strongly encouraged to participate in the relevant industry standards-setting processes.

To facilitate reliable interconnections, the Council developed a series of templates to identify issues parties seeking to interconnect should reach agreement on prior to interconnection. One template, the Network Interconnection Bilateral Agreement Template, provided four pages of issues designed to govern joint planning sessions between interconnecting service providers.[9] To facilitate the development of network interface standards and specifications, the Council developed a Network Interface Specification Template. It identified the minimum list of items that must be effectively addressed by service providers to establish and maintain points of interconnection, including such things as environmental operating requirements, power and grounding requirements, diversity requirements, interference protection levels, synchronization and timing requirements, *etc.*[10] To assess the reliability of new technologies, the Council developed a New Technology Reliability Template. The Template is designed to enable both service providers and equipment suppliers to evaluate issues raised by the integration of new technology into networks.[11]

Because the Council completed its work before the passage of the Telecommunications Act of 1996, the specific provisions of the Act were not reflected in the Council's report. In generally discussing developing telecommunications and information technologies, the report made this observation: "When it comes to development, information technology today is in its infancy. . . . if we've learned anything from the development of (new) technologies, it's that growth will be wild and chaotic and what ultimately happens will defy anyone's prediction."[12]

2.1 MISSION AND CHARTER

[8]The Path Forward, Increased Interconnections, at p. 71.

[9]The Path Forward at Increased Interconnection, pps. 50 - 54.

[10]The Path Forward, Increased Interconnections, at pps. 55 - 56.

[11]The Path Forward, Changing Technologies, at pps. 63 - 64.

[12]The Path Forward, Increased Interconnections, at p. 14.

The charter and the name of the Council were changed in April of 1996.[13] The primary charge made to the Council in its 1996 charter was to advise the Commission on what steps are necessary to implement new Section 256 of the Telecommunications Act of 1996. The charter is closely patterned after Section 256 and states that the Council's purposes are to provide recommendations both to the FCC and to the telecommunications industry that will assure optimal reliability and interoperability of, and accessibility to, public telecommunications networks. Specifically, the Council was asked to:

(1) identify, and prepare recommendations to avoid, barriers to interconnectivity, interoperability and accessibility of public telecommunications networks; barriers to the use of telecommunications devices with those networks, and recommendations to ensure seamless transmission between and across those networks;

(2) provide recommendations on how the Commission most efficiently can conduct effective oversight of coordinated telecommunications network planning and design;

(3) provide recommendations on how the Commission most efficiently can participate in the development by appropriate industry standards-setting organizations of public telecommunications network interconnectivity standards that promote access to telecommunications networks, to information services by subscribers of rural telephone companies, and to network capabilities by individuals with disabilities.

(4) continue to report on the reliability of public telecommunications network services in the United States.

2.2 NETWORK RELIABILITY AND INTEROPERABILITY COUNCIL

To perform the analysis and help develop the recommendations requested by the FCC, the Council decided at its July 15, 1996 meeting to organize two focus groups, to be staffed by volunteer subject matter experts. The experts were drawn from the various communities represented on the Council but also included experts representing other points of view the focus groups believed important to the work. The groups were organized along the lines established in Section 256: Focus Group 1 was asked to focus on network issues, and Focus Group 2 was asked to focus on standards issues. Specifically, Focus Group 1 was asked, first, to determine what are the technical and engineering barriers to network accessibility and interconnectivity and what should be done to overcome those barriers, and, second, what procedures should the FCC establish to oversee coordinated network planning.

[13]The Charter of the Council is attached as Appendix D.

Focus Group 2 was asked to review telecommunications standards-setting processes, and develop recommendations on what role the Commission should take in participating in industry standard-setting activity, particularly relating to access to networks, access to information services by subscribers of rural telephone companies, and access to network capabilities and services by individuals with disabilities.

To continue to report on the reliability of public network services, the Council decided to continue to rely on the ATIS Network Reliability Steering Committee, as it had for the past four years.

2.2.1 Focus Group 1: Network Connectivity and Planning Oversight

2.2.1.1 Study Process and Data Collection and Analysis

To accomplish its work, Focus Group 1 first developed a questionnaire to solicit expert opinion on what barriers exist or might develop regarding network accessibility and interoperability. More than 200 individual responses were received from a wide variety of participants. The responses were shared with Focus Group 1 team members, who were asked to respond. The resulting collection of barriers and issues were wide ranging and varied in their level of detail.[14] The issues were grouped under four headings that were deemed appropriate for common study and four teams were organized to focus on these issues.

The Planning Group was organized to consider planning issues, and to develop recommendations for the Council's consideration on what procedures the FCC should use to oversee coordinated network planning of telecommunications networks. Issues identified as being important in the data survey included identifying the differences between network planning and network implementation; identifying the key activities in network planning; determining the need for new institutions; and evaluating network and feature deployment issues.

The Implementation Group was organized to focus on implementation issues. The group focused on identifying and developing tools that are needed by networks seeking to interconnect. In particular, it sought to identify, and remedy, areas where information could avoid barriers to interoperability.

The Operations Group addressed operations issues identified in the data survey as impeding interoperability. In particular, it investigated the accessibility of operations support systems, performance monitoring, security requirements, signaling systems considerations and recommendations for interoperability testing.

The User Interoperability Group focused on barriers to accessibility by users of network services, including large, institutional users and private networks. The group considered such things as

[14]The list of barriers is included at Appendix E.

Internet connections, access to various high speed network services, and Customer Premises Equipment issues.

Although the four groups worked on assigned issues independently, they also met together at regular intervals. The Focus Group and its various teams made extensive use of electronic resources in accomplishing its work. These included an email reflector that enabled all members of the Group to communicate and a "home page" made available to the group by the FCC. Work product was posted at the home page as it developed, and commenters were able comment to the authors of the work electronically.

2.2.1.2 Team Members and Contributors

John Gunter, Chairman	BellSouth

Planning Task Group Members

Tony Pupek - Leader	Bell Atlantic
Greg Theus - Scribe	GTE Telops
Paul Hart	USTA
P.J Louis	NextWave Telecom
David Mangini	SNET Mobility
Tom Aprille	Lucent Technology
Peter Budihardjo	Nortel
Art Prest	CTIA
Richard Scharfenberg	SBC
Lee Wollgast	ICG
Bill Pennington	DSC
Larry Tiedt	GTE

Implementation Task Group Members

Andy Scott - Leader	NCTA
Suzanne Ford - Scribe	Time Warner
Pat Carstensen	Nortel
Dan Nielsen	US West
Jane Kimble	NYNEX
Tim Mack	Ameritech
Susan Miller	ATIS
Chuck Norman	Sprint
Randy Hudson	BellSouth

Operations Task Group Members

Louis Scerbo - Leader	Bellcore
Dick Dodd - Scribe	OSS Access Chair, BellSouth
Reinhard Metz	Signaling Co-Chair, Lucent
Fred Skoog	Signaling Co-Chair, DSC
Gene Phillip	Performance Monitoring Chair, NCS

Hank Kluepfel	Security Chair, SAIC
Pete Shelus	Interoperability Testing Chair, AT&T
Peter Budihardjo	Nortel
Royce Davis	GTE
Bill Young	MCI
Fred Tompkins	NCSA

Additional Operations Task Group Contributors

Ed Pinnes	Bellcore
Harold Daugherty	ATIS
Barry Lewin	Bellcore
Fred Kaudel	Desk Net
John Kimmons	Bellcore
Craig Tystad	Time Warner
Jeff Copley	DSC
Bill Hagerman	Lucent
Mike Megrew	Lucent
Dave Slade	Lucent
Rick Harrison	Bellcore
Judy Marcopulos	BellSouth
Mel Sobotka	Booz-Allen Hamilton
Pat McGreggor	NYQUTEK
Don Withers	Bell Atlantic
Richard Chatam	BellSouth
Eleanor Binderman	BellSouth
Alex Hood	BellSouth
Cheryl Wilcoxen	Intermedia Communications
Jack Davidson	Intermedia Communications
Fred Herr	NCS
George Caldwell	Frontier Corporation
Jaton West	Booze-Allen Hamilton
Dave Marshall	Bellcore
Kevin J. McMahon	MCI

User Interoperability Task Group Members

Bill Blatt - Leader	Nortel
Paul Lambert - Scribe	Compuserve
Vince Alesi	NYNEX
Dennis Corey	ATSI
Ken Hayward	Nortel
Ostap Monkewich	Nortel
James Kukla	Lucent
Karl Rauscher	Lucent
Walt Mansell	Shiva
Don Mulder	US Robotics

Nguyen Nguyen	NCS
Louis Rubin	Bellcore
Mark VanWert	Time Warner
Willie Woodmore	SBC

2.2.2 Focus Group 2: FCC Role in the Standards Setting Process

2.2.2.1 Study Process and Data Collection and Analysis

To accomplish its work, Focus Group 2 began by identifying and discussing questions raised by the standards provisions in Section 256. It formed four work functions as a result of its analysis.

Because NRC II had done a considerable amount of work addressing the role of the telecommunications standards-setting processes in establishing the reliable interconnection of networks, it first decided to review and evaluate that work from the perspective of Section 256. It would identify where extensions to the work were appropriate, and provide those extensions.

Second, it decided to assess all aspects of the telecommunications standards-setting process from the perspective of the statute. The review included documenting how standards development processes and organizations interrelate, and identifying how processes could be improved. It determined to review the historic relationship between that process and the FCC, to evaluate the effectiveness of that relationship in achieving the goals of Section 256, and to determine whether and how the relationship could be made more effective.

Third, the Group identified a separate work effort to focus on the performance of standards development processes in ensuring access to telecommunications services by individuals with disabilities. The Group determined to establish how, and from whom, standards organizations learn of special requirements by this community, and what role the FCC should play in this process.

Finally, the Group identified a work effort to explore the role of standards-setting organizations in providing access to information services by persons in rural areas, and to identify what role the FCC should play.

Focus Group 2 worked as a team on each issue, with different members serving as leaders for particular issues. The Group made heavy use of electronic facilities, including an electronic mail reflector and an electronic "home page," both of which were provided to the Group by Committee T-1 and its support organization, the Alliance for Telecommunications Industry Solutions. The Group met throughout the study period both in person and by telephone conference calls.

2.2.2.2 Team Members and Contributors

Jerry Peterson, Chairman	AT&T and Committee T-1
Rick Canaday	AT&T

Dan Bart	TIA
Trent Boaldin	Elkhart Telephone
Steve Barclay	ATIS
Harold Daugherty	ATIS
Mel Woinsky	Nortel
Charles Bailey	SBC
Jim Baskin	NYNEX
Dennis Bodson	NCS
John Bobsin	Lucent
Charles Elderling	NextLevel
Larry Young	Ameritech
Rick McNealy	BellSouth
Roger Nucho	Bell Atlantic
Barbara O'Connor	Alliance for Public Technology
Martin Singer	Motorola
Jim Eitel	US West
Scoop Sairanen	TCA
Bill Pennington	DSC
Raju Patel	NextWave
Art Reilly	Bellcore
Scott Bradner	Internet Society
George Dobrowski	ATMF
Bill Stipe	ALTS
Ahmed Patel	MCI
Ollie Smoot	IISP/ITI
Susan Bober	TCA
Mike Brusca	NYNEX
Peter Lefkin	IISP
Jenifer Simpson	National Cerebral Palsy Foundation
Mitesh Patel	IISP

2.3 NETWORK RELIABILITY

Wireline telephone companies are required to report to the FCC outages that meet certain parameters, the most common being telephone service outages that significantly degrade the ability of more than 30,000 customers to make a call for more than 30 minutes.[15] In establishing reporting requirements, the Commission stated it was concerned that it did not have a systematic means by which to monitor major telephone service outages throughout the nation on a timely

[15]The Commission's outage reporting rules are at 47 C.F.R. Sec. 63.100.

basis. It also was concerned that information about vulnerabilities be shared, and it encouraged industry organizations to participate in the information sharing.[16]

The first Network Reliability Council proposed certain modifications to the FCC's outage reporting criteria among its conclusions and recommendations addressing the causes of and mitigation steps for outages. It also determined there should continue to be a cross-industry group of experts monitoring and analyzing the service outage data reported to the FCC. It proposed the organization that now is the Alliance for Telecommunications Industry Solutions organize that effort.

The Network Reliability Steering Committee (NRSC) was established by ATIS in response to the request. The group's mission statement provides that it is a consensus-based committee, organized to analyze the telecommunications industry's reporting of network outages. The purposes of the analysis are threefold: (1) to identify trends in network reliability; (2) to distribute the results of the analysis to the industry; and (3) to refer matters to appropriate industry forums for further resolution, where necessary. The objective of this work is to ensure a continued high level of network reliability.

NRC II and the Network Reliability and Interoperability Council relied on the NRSC to monitor, and report on, network reliability. The NRSC makes presentations at each of the Council's meetings.

The NRSC has continued to analyze outage data largely according to the categories established by NRC I. These categories are facility outages, switch outages (local and tandem), signaling network outages, central office power outages, overload (congestion) outages, natural disaster outages, and outages resulting from other causes. The group has established control charts around each category to compare new outages with outages that occurred in the first (baseline) year of reporting. The group regards outages outside established tolerance limits as of concern and in need of action. To improve the rigor of its analysis, the group also uses a metric established by Committee T-1 to measure the relative impact of an outage on the public. The metric was not available to NRC I, but the NRSC has used the index retroactively to evaluate all reported outages.[17]

The overall conclusions are that based on the frequency of events and the impact of the events using the outage index, the overall reliability of networks has remained constant. Areas of concern have been studied, including the frequency of power-related outages, but the single largest area of concern continues to be outages that result from damage to facilities, primarily damage to fiber optic transmission cable. The group has published a study on these incidents, which concludes that more than 50 percent of facility outages are caused by construction activity that damages underground fiber optic cable ("dig-ups"), and that more than one-half of these

[16]FCC CC Dkt. No. 91 - 273, paras. 4, 32 (February 27, 1992).

[17]Committee T-1 - Telecommunications, Technical Report No. 42, "A Technical Report on Enhanced Analysis of FCC-Reportable Service Outage Data," August, 1995.

incidents occurred because the excavator either failed to notify the facility owner or failed to provide adequate notification. The NRSC finds, as did both NRC I and II, that the most effective solution is legislation that requires excavators to notify facility owners before they engage in construction. The group finds that states that have weak laws in terms of coverage or enforcement have the highest incidents of service outages resulting from such damage. It states the telecommunications industry is united in its support for comprehensive and effective one-call legislation as a means to improve network reliability, but to be successful, there must be strong, consistent and broad-based support from all industries and associations affected, including federal agencies and congressional leadership.[18]

The Network Reliability and Interoperability Council continues to call for the passage of comprehensive federal one-call legislation with adequate enforcement mechanisms and minimal exceptions as the most effective way for the nation to enhance the reliability of its telecommunications service. The members of the Council are available to provide their assistance in this effort.

[18]"Keeping the Network Alive and Well," Network Reliability Steering Committee (ATIS, February, 1996), pps. 1, 11, 14-15.

3. TELECOMMUNICATIONS ACT OF 1996

The Telecommunications Act of 1996 was passed by the Congress to establish "a pro-competitive, deregulatory national policy framework" for the United State's telecommunications industry.[19] Specifically, the Act states in its title that it is "(a)n act to promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies." Many of its provisions add to or otherwise amend existing provisions of the Communications Act of 1934, and have led the Federal Communications Commission to commence more than 70 notice and comment rulemaking proceedings .

The Act is comprehensive, and many of its provisions interrelate. Before beginning a notice and comment rulemaking proceeding relating to Section 256, titled "Coordination for Interconnectivity," the Commission asked the Network Reliability and Interoperability Council for its views on what findings and recommendations it could offer in determining how the purposes of Section 256 could best be accomplished.

3.1 FRAMEWORK ESTABLISHED BY SECTION 256 AND RELATED SECTIONS

Section 256 of the Telecommunications Act of 1996 (see Appendix A) has four subsections: (a) Purpose, (b) Commission Functions, (d) Commission's Authority and (d) Definition. The stated purposes of Section 256 are:

(1) *To promote nondiscriminatory accessibility by the broadest number of users and vendors of communications products and services to public telecommunications networks used to provide telecommunications services.*
(2) *To ensure the ability of users and information providers to seamlessly and transparently transmit and receive information between and across telecommunications networks.*

The Act also prescribes how the first purpose shall be accomplished:

A) Through *coordinated public telecommunications network planning and design by telecommunications carriers and other network providers of telecommunications service* and
B) Through *public telecommunications interconnectivity, and interconnectivity of devices with such networks used to provide telecommunications service*.

[19]S. Conf. Rep. No. 104-230, 104th Cong., 2d Sess. 1 (1996) ("Joint Explanatory Statement").

Under subsection (b) the Commission is given two functions, one mandatory (the Commission shall) and the other permissive (the Commission may). The Commission is mandated to *establish procedures for Commission oversight of coordinated network planning by telecommunications carriers and other providers of telecommunications service for the effective and efficient interconnection of public telecommunications networks used to provide telecommunications service*. The Commission is permitted (but not required) to *participate, in a manner consistent with its authority and practice prior to the date of enactment of this section, in the development by appropriate industry standards-setting organizations of public telecommunications network interconnectivity standards that promote access to:*

(A) public telecommunications networks used to provide telecommunications services,
(B) network capabilities and services by individuals with disabilities,
(C) information services by subscribers of rural telephone companies.

In subsection (c), the Act emphasizes that this section (256) neither expands nor limits the Commission's authority under law prior to the Act.

In subsection (d), public telecommunications network interconnectivity is defined as *the ability of two or more public telecommunications networks used to provide telecommunications services to communicate and exchange information without degeneration, and to interact in concert with one another*.

Other definitions should also be noted. The phrase *public telecommunications networks used to provide telecommunications services* is used several times in this section. The term *Telecommunications*, defined at Section 3(43), means the *transmission, between or among points specified by the user, of information of the user's choosing without change in the form or content of the information as sent and received. Telecommunications Service* means *the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used*. Although the term 'public telecommunications network' is not defined by the Act, *Telecommunications carriers* means *any provider of telecommunications services*. Section 3(44) further states that *A telecommunications carrier shall be treated as a common carrier under this Act only to the extent that it is engaged in providing telecommunications services.*

In Section 251(a), the Act (see Appendix B) specifies the two duties of each telecommunications carrier. The first duty is *to interconnect directly or indirectly with the facilities and equipment of other telecommunications carriers*. The second is *not to install network features, functions or capabilities that do not comply with the guidelines and standards established pursuant to Sections 255* (Access to Persons with Disabilities) and 256 (Coordination of Interconnectivity).

The members of the Council believe that, if the overall purpose of the Act, as stated in its title, (*To promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies*) is to be achieved in a manner consistent with the second duty of each telecommunications carrier under Section 251(a), it is critical that

the guidelines and standards established under Sections 255 and 256 not be unduly restrictive or limiting on the industry.

A key operating assumption of the NRIC members is that Congress envisioned a telecommunications market with a rich range of telecommunications services each of which satisfies some telecommunications consumers' needs and is offered in a fully competitive marketplace by service providers at an equally broad range of prices intended to attract customers. It is also assumed that the FCC's function is intended to be that of a facilitator in the creation of an environment in which a telecommunications consumer could choose from a number of providers to receive telecommunications services and that, once the consumer's choice had been made, those providers would provide technical cooperation to each other as necessary to meet the consumer's needs and expectations.

It appears that Congress did not anticipate that market forces alone would be sufficient to drive the level of cooperation it believed necessary. Only telecommunications carriers -- but all telecommunications carriers -- are subject to Section 251(a). Sections 251(a), 255 and 256 place unique expectations and obligations on these service providers. Justification for these unique requirements may be based on historical experience. Some commentators attribute the absence in the early part of this century of a legal requirement of common carriers to interconnect to be the primary factor in the development of monopolies[20] Expert commentary also supports such requirements. Many economists believe that market forces will result in islands of very high interoperability within telecommunications networks but lower levels of interoperability across networks, as service providers seek to capture the value of network effects.[21]

The Council believes that "seamless" interoperability must be perceived from the user's perspective. "Seamless" interoperability should be interpreted in terms of the consumers' perceptions when they acquire and use the services they desire. This encompasses two different kinds of interoperability. The first and most obvious is facility and equipment interoperability that enables a user of one carrier's network to communicate with a user of another network without being aware that more than one provider's network is being used. The second kind of interoperability requires provisioning processes that enable consumer's requests to one provider for service (that uses multiple providers' facilities) to be coordinated among the involved providers so that the consumer's expectations are met in a timely, quality fashion.

Consumers have a right to expect their overall service, however constructed, will meet their needs and that all their service providers have a joint responsibility to ensure that those needs are met. Interoperability in telecommunications historically has been made possible through

---

[20.] Federal Telecommunications Law, M. Kellogg, J. Thorne, P. Huber, p. 12 (1992); Behind the Telephone Debates, C. Weinhaus and A. Ottinger p. 9 (1988).

[21.] Islands in the Bit Stream: Charting the NII Interoperability Debate. F. Bar, M. Borrus, R. Steinberg, available on the Internet at:

http://www-leland.stanford.edu/~fbar/inter.html

interfaces defined by the voluntary standards-setting process. However, seamless interoperability does not necessarily require a single industry standard. Rather, it requires, for example that (a) interconnecting carriers must provide conversion technologies when transmission protocols are different and that manufacturers must provide adapters or converters to enable interconnection where equipment interfaces differ, (b) that bilateral agreements between interconnecting carriers are established based on industry standards, or (c) that a single industry standard exists.

The interconnection of disparate networks is not a new phenomenon. Today, wireline network users communicate with wireless network users. What is new about the interconnection of multiple networks under TA96 is that the interconnecting parties can compete directly for the same user. The difference is one of relationships, not of technology or standards.

Section 256 does not seem to call for an improved level of interoperability than exists today among telecommunications networks, nor does it seem to call for a greater level of access to these networks. Rather, its focus seems to be prospective, and its primary concern that changes fostered by TA 96 not interfere with its goals.

It is worthwhile to briefly review selected recent history regarding the impact of change within the telecommunications industry, and how end users dealt with any barriers or issues that were subsequently created. Following the implementation of the Communications Act of 1934 and proceeding through the early 1970's, the telecommunications network was largely seen by end user as "the telephone company." There were few choices for access options, CPE was provided by the telephone company, and network interconnections were carefully managed, largely by the Bell System.

The first significant change came when it was determined that end users could connect their own CPE, as long as the CPE conformed to new FCC rules put in place to protect the network from harm (generally referred to as FCC Part 68 rules). End users now had the option of connecting their own devices, but were faced with new technical/engineering issues such as how to connect an RJ-11 based device into home wiring previously based on four-pronged connectors, or determining the number of devices that could be supported by the inside wiring scheme. The competitive telecommunications market responded to these new needs by supplying a number of solutions, such as home wiring kits and connector adapters, among many others. The market also responded to needs for other new communications products which could interconnect, such as answering and fax devices. Not all solutions were perfect, not all solutions interoperated with all other solutions -- but the competitive forces that drive all markets worked within the telecommunications market -- solutions that didn't work faded away, new solutions were constantly introduced, and so on. It should be noted that the fax industry, for example, without any intervention or help from regulatory agencies, responded efficiently to consumer pressures for full interoperability.

Other market conditions drove end user learning curves, such as newly introduced fees for CPE or home wiring maintenance. End users had the choice to trouble shoot their own problems or pay the telephone company to do so. Again, the resulting barriers seemed to melt in the face of competitive force and consumer choice. It should be noted that the FCC did provide guidelines

for network-to-CPE connection. CPE made available for use in the U.S. must meet those requirements (Part 68), and networks must provide a compliant point of interface. The purpose of the FCC's rules, however, was to avoid harm to the networks; it was not to achieve "seamless interoperability."

The introduction of new long distance companies also created new issues for end users. Such issues as how to choose a long distance carrier, coping with new dialing schemes and post-dial delay, use of touch tone vs. pulse, and having to deal with multiple bills cropped up. Once again, new end user needs were effectively addressed by the competitive market. Telecommunications consultants appeared en masse, willing to help end users make choices, new CPE was introduced to support longer memorized dialing schemes, modem scripts supported end user defined timing and multiple dialing streams on single calls, and so on. As with Part 68, the FCC and the courts needed to resolve some issues, but for the most part issues of interoperability were resolved through private processes.

The development and deployment of equal access required new learnings by consumers, but the end user seems to have survived quite well. In retrospect, some solutions worked while others did not. Interoperability was largely achieved, but it was not "seamless" in every sense and occurred because the end users made it a condition of success for competitive entrants. FCC rules for equal access dialing provided more competitive conditions for new long distance carriers and made it easier for end users to access those carriers, but interoperability was not greatly impacted.

Cellular networks emerged during the 1980's, giving end users more ways to access telecommunications services. Evolution within the wireless market has led to the further development and deployment of digital cellular and other PCS technologies. As expected, the end user had new issues -- what wireless CPE to buy, keeping wired service as well as wireless, dialing before dialtone and hitting a "send" button, compatibility with portable computing and modem solutions, among others. The evidence so far is that the competitive market is dealing with these issues as networks and service providers strive to gain and retain more end users. End users understand that wireless and wireline CPE are not interchangeable, and they make choices accordingly. Wireless CPE which works on one network may not work on another, but consumers seem to understand this and make service provider/CPE choices which suit their needs (wireless CPE providers are already addressing the incompatibility of certain CPE-network combinations by making handsets which will work on multiple networks built with different technologies). End users are comfortable that a voice call made on a wireless network will complete to any other end user on any other type of network. If end users demand strongly enough that successful entrants must provide CPE that works on any type of network, it will happen. Until then, some solutions will interoperate, some won't, old solutions will disappear and new solutions will emerge, all based on end user demand for some level of interoperability. This interoperability will not, however, be "seamless" in every sense of the word.

Services are widely available across many different types of networks. Telecommunications answering services, for example, range from rerouting calls to humans, wired answering devices, voice mail associated with the terminating network, voice mail based on end user defined

routing, *etc.* These voice mail systems do not interoperate with each other, but they do terminate basic voice calls from any type of originating network. Should the fact that an end user must know how to leave messages in a number of different ways be considered a barrier to access or interoperability? Should these systems be forced to interoperate “seamlessly”? The Council believes that while almost any new service or CPE offering could be construed as introducing new technical or engineering barriers for end users, it is our opinion that a competitive market place is generally sufficient to resolve those issues, and that the time required for new products and solutions to emerge and reach some level of maturity with end users should not be construed as "non-interoperable," "non-seamless" or “non-transparent.”

Competitive markets thrive when given an opportunity to respond to the demands of paying customers, but it must be recognized that some end users will make choices that do not survive, and for these end users the experience will not appear to be seamless. We believe that end users increasingly will have more choices when selecting a telecommunications carrier for everything from basic voice access to high speed data access, from wireline to wireless, from local to long distance, bundled in as many ways as one can imagine. CPE choices will proliferate, from ISDN to ADSL, from analog to digital, and so on. But to believe or expect that all new competitive offerings will "seamlessly interoperate" with all other new offerings or with existing CPE is not realistic.

Despite the Council's conviction that a competitive market provides a sound and effective way to deal with most end user barriers that might emerge under the Telecommunications Act, we also recognize that some universal expectations do exist on the part of end users - namely, that certain services will work largely as they have in the past. These expectations are based largely on history, and relate to common service definition.

A common service definition (see also Service Requirements/Definitions in Section 4, Interoperability Planning) refers to the notion that end users have some nationally accepted expectations regarding the way certain services may be accessed or what they mean. While one can debate at length whether these expectations are appropriate or whether they were arrived at as a result of competitive forces, they nevertheless exist. We refer to such things as a simple POTS call, 800 (and now 888) being toll free calls which can be dialed from virtually any type of originating network, delivery of caller ID information, and soon such services as Local Number Portability. A unilateral action by a telecommunications carrier which would prevent access to these services, or an action which would cause these services to be non-functional in a backward compatible manner for end users who have taken no action would fall short of the reasonable expectation for seamless interoperability. A list of such national services would be very small.

For example, suppose a new telecommunications carrier, after signing up many thousands of new customers in a comparatively acceptable manner, unilaterally decided to introduce new caller ID capabilities in a way that departed from existing conventions and which would require all of the service provider’s customers to purchase a new CPE just to maintain the capabilities that existed before, even if the end user does not want to purchase the new capability. One might argue that such an action, in the spirit of competition, is acceptable because end users would have the choice of buying service from a competing service provider. However, such forced

inconvenience could easily disrupt end users in more significant ways than just having to look somewhere else for service. End users may have business or personal practices which are dependent on such services, and even originating callers may be depending on the terminating caller to have the original capabilities.

The Council recommends that the FCC develop a short list of nationally accepted services and require that no telecommunications service provider make any system-wide changes in or extensions to such services that would cause a subscriber to lose such services unless those changes or extensions (1) are the product of the National Planning Process discussed in Section 4 below and (2) provide an opportunity to the customer to maintain uninterrupted service.

It is recognized that the FCC may add services in the future should there be a compelling national need which the industry would not be able to respond to in a voluntary manner. The planning model for national services, as outlined by the Planning Task Group, should be used to reach industry-wide consensus on any changes once services are on the FCC's list. Of course, service and network providers should be free to work with specific end users to introduce changes in a competitive and voluntary way, even if new CPE or other requirements are placed on the end users. Such services are depicted by the Planning Task Group as regional/proprietary.

The Council also considered the issue of how end users can appeal when they are not satisfied that their telecommunications carrier or CPE has met the goal of “seamless interoperability.” We believe that in the highly competitive environment envisioned and encouraged within the Telecommunications Act, end users will have sufficient choices in these areas to drive providers to maintain high levels of customer satisfaction or risk losing their customer base. In cases where a failure to meet interoperability requirements causes harm to an end user, there will continue to be processes at the local, state, and Federal levels to address and resolve those issues. Examples of such processes include legal proceedings, appeals to public utility commissions, and appeals to the Federal Communications Commission.

4. INTEROPERABILITY PLANNING

In response to Section 256 of the Telecommunications Act of 1996, the Planning Task Group (PTG) under NRIC Focus Group 1, worked to develop recommendations to the FCC as to how it might best accomplish responsibilities placed on it by that section. Among the recommendations requested were those pertaining to how the Commission most efficiently could conduct effective oversight of coordinated telecommunications network planning and also, how optimal reliability and interoperability of the public telecommunications networks will be assured. Based on the perceived technical barriers to the interconnection and accessibility of networks that were submitted by industry experts (see Appendix E), there were three groupings of the barriers related to Planning: (1) Competitive and Sensitive Information, (2) Forecasts and Joint Planning, and (3) Future Network Architectures. Using the list of barriers provided and identifying others, the PTG pinpointed a set of *Key Issues* to study in their effort to produce the necessary recommendations.

Those *Key Issues* are:

1. Identify the differences between the planning of network architectures and network implementations (*e.g.,* SONET vs. ring deployment).

2. Identify the differences between the planning of national and regional services (*e.g.,* 800 Service vs. voice messaging).

3. Examine the transition of architectures, products and services from a proprietary to a public status.

4. Determine kinds of activities of existing industry forums (*e.g.,* ATM Forum, CLC, *etc.*) in the planning of products and services and explore the need for new forums.

5. Evaluate the impacts that protecting competitive information has on the planning and design of products and services.

6. Examine timing issues relative to matching the availability of network products and services to users and vendors needs.

7. Develop a recommendation on the FCC's role for coordinated network planning.

Either individually or as a team, members of the PTG championed investigations of the *Key Issues* and white papers were prepared. The information contained in the write-ups was used in PTG discussions to further understand the significance of each issue relevant to the planning of telecommunications products and services in today's environment, and the extent of coordination latent among telecommunications carriers and other providers of

telecommunications services. Quickly, a close linkage between all of the *Key Issues* was realized and it was evident to the PTG that a process model would best serve in portraying network planning, design, and implementation activities. Further, a process model could accommodate both existing and deficient activities, readily depict telecommunications industry participants' roles and responsibilities, identify distinct hand-offs to other processes or activities, and support multiple processes and a transition capability from one to the other.

The **Services Planning Process Model,** shown as Figure 1, was developed by the PTG to use as the foundation for the recommendations presented in this report.

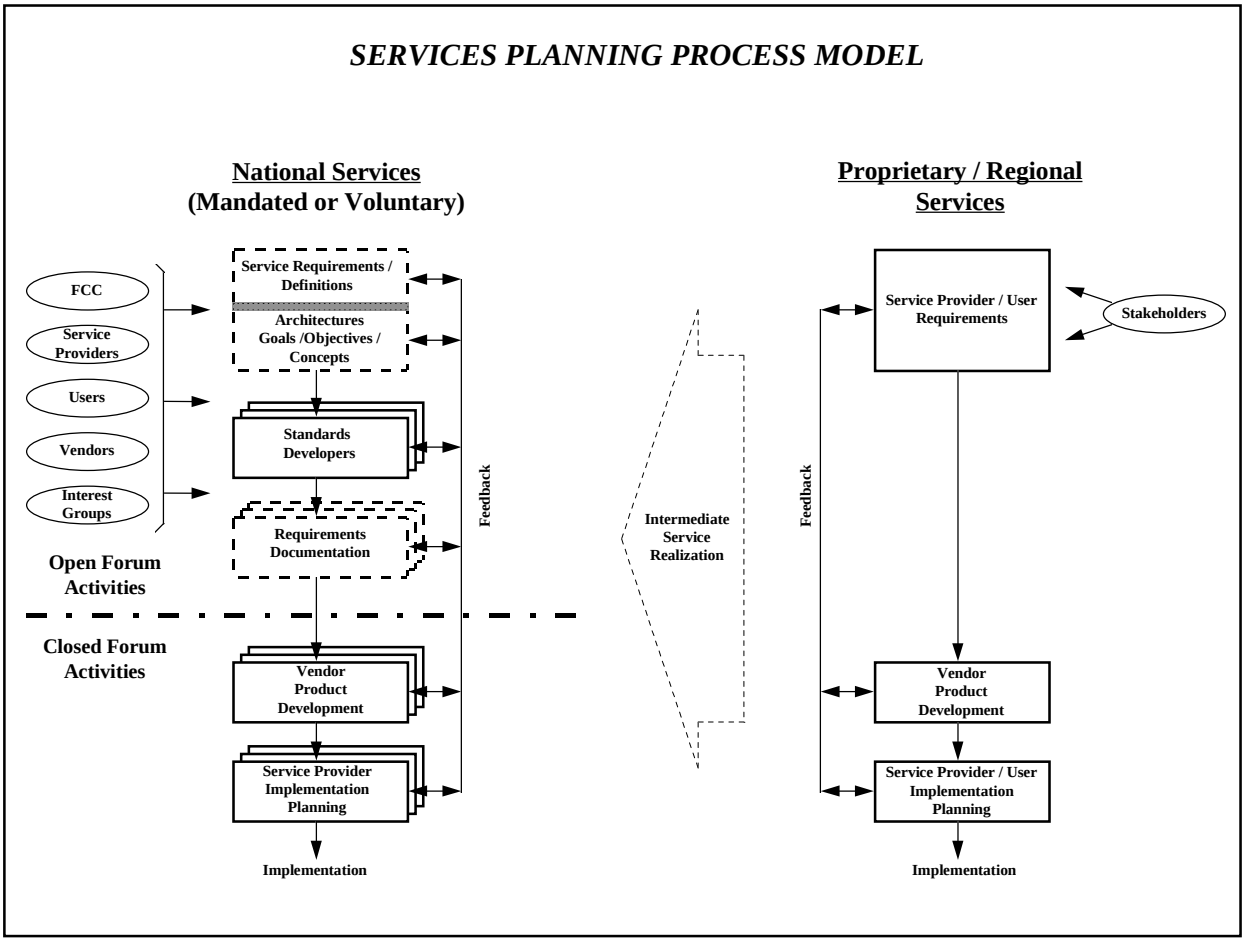


FIGURE 1.

The following is a high level description of the Services Planning Process Model (SPPM):

There are three significant developments that make up the SPPM. Two of these are distinct process flows; one flow was developed for National Services (Mandated or Voluntary) and the other for Proprietary / Regional Services. The third development is the *Intermediate Service Realization*, a transition capability, which is the potential linkage between the process flow for National Services and that for Proprietary / Regional Services.

The process flow for National Services is divided into activities performed either in "Open Forum" or in "Closed Forum" because generally, National Services require extensive planning and coordination of activities to the point where development begins. Among other things, the industry's competitive environment suggests the need for this division of activities, but the opportunity to cooperate and share throughout this process flow is highlighted by the presence of feedback loops between all of the activities. This process begins with activities that require close linkage, *Service Requirements / Definitions* and *Architectures Goals / Objectives / Concepts.* The dotted box is typically representative of a need to define or redefine, some or all, of the activities depicted in the process flow. In the next step, *Standards Developers*, a set of activities takes place, for the most part as they do today and going forward as recommended by Focus Group 2 (see Section 9). However, requirements meeting interoperability criteria should be explicit and through activities occurring in *Requirements Documentation* (an intended activity), that formality is provided. Participation in the National Services process through the aforementioned steps is unrestricted and portrayed as a cooperative effort of Service Providers, Manufacturers, Users, Regulatory Bodies, Interest Groups[22], et al. There are two activities, *Vendor Product Development* and *Service Provider Implementation Planning*, that complete the planning process for National Services. Both activities are shown as "Closed Forum", which is not a departure from the way they are currently performed. As business issues dictate, vendors (manufacturers) will build and offer products that are based on standards and readily available requirements documentation. Implementation Planning activities, contrary to those of Architecture Planning, take place between individual service providers or between an individual service provider and their chosen vendor(s) and as such are not generally performed as "Open Forum" activities. National Services planning activities end with *Service Provider Implementation Planning*; afterwards actual Implementation, or deployment activities commence.

The National Services process flow accounts for but one of the two significant categories of services that are provided over public telecommunications networks. To handle what is deemed as the other significant category, the Proprietary / Regional Services process flow was developed. In contrast to the planning of National Services, and because service characteristics do not have to exactly be the same, all of the process activities for Proprietary / Regional Services will, as they are currently, generally be performed within the confines of the service providers and their chosen vendor(s). Therefore, this process flow is initiated around *Service Provider / User Requirements* activities that, for practical purposes, are business driven and open to stakeholder's input. As with the National Services process flow, *Vendor Product Development* and *Service Provider Implementation Planning* activities are present. However, the requirements that drive these activities are not necessarily based on industry standards and the resulting products and services are not expected to be implemented or function with the same degree of

[22]"Interest Groups" include, but are not limited to, such telecommunications associations as the United States Telephone Association (USTA), the Cellular Telecommunications Industry Association (CTIA), the Personal Communications Industry Association (PCIA), the Telecommunications Industry Association (TIA), and the National Cable Television Association.

interoperability as National Services. Additionally, like the National Services process, the planning process of Proprietary / Regional Services necessitates the use of feedback loops throughout to be effective. These planning activities conclude, as they did with the National Services process, with the actual Implementation, or deployment.

The third development of the SPPM, *Intermediate Service Realization,* is representative of the transition capability to be applied when the planning process needs to evolve from that for a Proprietary / Regional Service to that for a National Service. Flexibility should be part of the evolution process since the need to transition may occur at any point during the process flow. Following the transition, the full extent of the National Services process flow, with its increased industry participation requirements, will control.

Conclusions reached by the PTG and excerpts from the *Key Issue* white papers are shown below as Key Learnings which were instrumental in the building of the SPPM and formulating the list of Recommendations.

4.1 NETWORK ARCHITECTURE PLANNING VS. NETWORK IMPLEMENTATION PLANNING

4.1.1 Key Learnings

The activities considered part of planning of network architectures[23] and the activities considered part of planning of network implementations are different and distinct. Accordingly, this supports the premise that the planning of network architectures (and national services as discussed later in Section 4.2) requires heavy industry-wide interactions prior to and during the technology development phases, while the planning of network implementations entails activities that are generally performed and carried out by individual service providers or jointly, by agreement, between multiple service providers.

Generally, the activities associated with the planning of network architectures must be completed first and are carried out in answer to the questions, “What?” and “How?”. While the follow-up questions, “When?”, “Where?”, and “How-much?” are pertinent to the planning of network implementations, which takes place subsequent to the network architecture planning.

The effectiveness of the planning of network architectures is proportional to the number of industry participants, their level of involvement and understanding, and the degree of cooperation that is present during the process.

4.1.2 Recommendations

[23] Network architectures are defined as the infrastructure (core technologies, systems and components) which enables public networks to provide telecommunications services and products to users.

4.1.2.1 Participation in Planning of Network Architectures

The planning of network architectures, including *Architecture Definitions (Goals / Objectives / Concepts), Standards Developers,* and *Requirements Documentation* as shown on the Services Planning Process Model (Figure 1), should be performed by a field of industry participants that includes, but is not limited to, Service Providers[24] or their representatives, Equipment Suppliers, Regulatory Bodies[25], Industry Consultants, Users, Interest Groups, and anyone with a vested interest in telecommunications products or services. Additionally, since the ability to comply with network reliability obligations and interconnectivity requirements, and offer nondiscriminatory accessibility hinges on such participation, it should be encouraged.

4.1.2.2 Open and Closed Forum Activities

"Open Forum" activities are associated with the concepts of joint planning and information sharing and should be worked in a manner that is unrestricted and accessible to all interested participants. The activities shown on the Services Planning Process Model (SSPM) (Figure 1) for National Services including *Service Requirements / Documentation, Architectures Goals / Objectives / Concepts*, *Standards Developers*, and *Requirements Documentation* shall be considered "Open Forum" activities. On the other hand, the remaining "Closed Forum" activities are, for the most part, carried out by manufacturers, providers, and producers at their own discretion. The spirit of "Closed Forum" activities is aligned with business issues and as such, is not contradictory to the idea of interoperability since such activities are performed around accepted and adopted open industry standards and requirements.

4.1.2.3 Activities Considered Part of Planning Network Architectures

Specific activities in the planning of network architectures should be performed by the participants (see 4.1.2.1) and are considered "Open Forum" activities (see 4.1.2.2). The following list of activities is not all inclusive but is representative of the focus on the "What?" and "How?" for Planning Network Architectures:

- Selection of applicable technologies
- Identification of functional requirements of technologies
- Identification of points of open connection (see Section 9.4.2.2)
- Selection of technical standards for open interfaces
- Development of interoperability testing requirements
- Identification of applicable network support system requirements
- Identification of operational impacts

4.1.2.4 Activities Considered Part of Planning Network Implementations

[24] Service providers include the realm of suppliers of telecommunications products and services offered over public telecommunications networks (*e.g.*, LEC, IXC, CLEC, CAP, Cellular, PCS, Cable, Satellite).
[25] Regulatory Bodies, particularly the FCC, are expected to oversee the planning activities according to the recommendations set forth in this report.

Specific activities in the planning of network implementations should be performed by the Service Providers and their Vendor(s) and shall be considered "Closed Forum" activities (see 4.1.2.2). The following list of activities is not all inclusive but is representative of the focus on the "When?", "Where?", and "How-much?" for Planning Network Implementations:

- Equipment identification and deployment areas
- Equipment interconnection specifics
- Network dimensioning (*e.g.,* traffic engineering, capacity planning, *etc.*)
- Service option selection by Market Area
- Vendor product selection
- Economic evaluation of deployment alternatives
- Identification of budgetary requirements
- Vendor contract negotiations and placements
- Determine engineering criteria
- Develop and implement new or changed operating procedures
- Develop equipment forecasts
- Negotiate standard provisioning intervals

4.2 NATIONAL SERVICES PLANNING VS. PROPRIETARY / REGIONAL SERVICES PLANNING

4.2.1 Key Learnings

Planning for a new service that is intended or required to be deployed on a national or widespread basis in the national network is a major undertaking. The successful deployment of National Services (Mandated or Voluntary) requires extensive planning and coordination within the telecommunications industry. Inputs must come from service providers, vendors, users, regulators, interest groups and others that might be affected.

In the planning process for new services, both National and Service-Provider Specific, sometimes new capabilities will be fundamentally supported by architectural structures and elements that are already in place. Other times, new additions may be required, and in some cases, major architectural upgrades to the network will be necessary.

Planning for National Service deployment was done by AT&T pre-divestiture, and generally by the Bell Operating Companies (BOC) post divestiture. Planning typically includes evaluation of many architectural alternatives, and the effects on support functions including Operations support activities (see Section 6) as well as network switching and transmission elements. Historically, planning for new services included service and architectural asset planning as an integrated activity.

The telecommunications industry has minimal experience in planning and implementation of National Services in the environment contemplated by the

Telecommunications Act of 1996. It is essential that a framework for such activities be established and tested as new National Service needs are identified.

There are three general Service Categories:

A. Services that start out as mandated capabilities on a widespread or ubiquitous basis from the beginning. 800 Service per the FCC's Order in CC Docket No. 86-10 is an example. A potential future example is 500 number portability.

B. Services that started out as Proprietary / Regional (sub-national) and as a result of developments, have become national in scope. Local Number Portability (LNP) is an example which was initially ordered by state commissions in Illinois and Georgia and has evolved to become a National Service pursuant to the Telecommunications Act of 1996.

C. Services that began on a limited local basis, and while they may be deployed on a widespread basis, are not required to have similar characteristics. Voice Messaging and ISDN are examples. While certain of these service offerings may eventually demonstrate a number of similarities across the country, uniformity (interworking) has not been compelled by any regulatory requirements. To the extent that similarities exist, they may have come about as a result of common interest and individual service provider decisions dictated by consumer demand. National ISDN was developed voluntarily by the telecommunications industry, and proprietary versions of ISDN continue to operate.

It can be seen that Service Categories A and B above, are the same in the limit. When a service starts out as national in scope, as 800 Service did, it must be addressed as such at the outset. A service such as Local Number Portability (LNP) was local at inception, but became a national issue on issuance of the Commission's Order in CC Docket No. 95-116. From then on, LNP is handled the same as examples in Category A. Services in the Local Service Category C, are not currently under the Commission's oversight, and until and unless some formal action makes a service national in scope, the Commission plays no role in its planning or deployment, apart from regulations designed to assure equipment connected to the network does not cause harm (FCC Part 68 regulation).

4.2.2 Recommendations

4.2.2.1 Service Definition for National Services

The process for National Services planning should begin with the development of a service definition which provides the feature characteristics of the service. Included in the definition are details on the geographic scope as well as service provider scope[26] of the service.

[26] The intent of geographic scope is obvious, but service provider scope can vary widely. Some services may be mandated for a particular segment, *e.g.*, all LECs, but another segment, *e.g.*, Cellular, may not be required to offer

It also includes backwards compatibility requirements and the extent of interconnection and interoperability required for the service. As to level of detail, the service definition needs to be sufficiently specific to provide a planning basis that identifies all of the characteristics that must be achieved in practice as a result of completion of the implementation process.

4.2.2.2 Participation and Activities in Planning for National Services

The planning for National Services, like the planning for Network Architectures (see 4.1.2.1), specifically *Service Requirements / Definitions* as shown on the Services Planning Process Model (Figure 1), should be performed by a field of industry participants that includes, but is not limited to, Service Providers or their representatives, Equipment Suppliers, Regulatory Bodies, Industry Consultants, Users, Interest Groups and anyone with a vested interest in telecommunications products or services. Additionally, since the ability to comply with network reliability obligations and interconnectivity requirements, and offer nondiscriminatory accessibility hinges on such participation, it should be encouraged.

The proposed new environment presented in the Telecommunications Act of 1996, in regard to National Services planning, must fairly take into account all of the issues involved in the deployment of services on a widespread basis. Provisions must be made for functions known to be required such as specification development, trials and testing, and large scale interoperability testing when necessary. Effects of new services on support systems and the requirement that new network functions and services must not compromise the utility of existing services or network reliability must be established.

National Services planning should make use of the currently available structural resources[27] of the telecommunications industry and develop one additional function that would provide an overall coordination capability for the management of both planning and coordination activities. This new function should have the following characteristics:

1. The National Services planning and coordination function should be organized as part of the industry consensus process. It should accomplish many of the functions of a federal advisory committee, but should not be formally impaneled as such.

2. Each National Service should have its own dedicated planning and coordination

---

the capability. A major point, however, is that the service definition should include information that will permit network participants that may want to provide a service to be able to, regardless of whether they may be initially obligated to do so by regulatory fiat.

[27] It is clear that not every conceivable function that might be required is currently active. What is available within the ANSI-accredited structure and the industry consensus forum structure are all of the basic structural resources needed. If a new standard is required, and an ANSI-accredited activity is warranted, it can be accomplished in an existing forum or a new one can be initiated under the existing structure. If new issues requiring industry consensus arise, either existing structures can be utilized or new ones developed.

activity, managed by a service-specific group.

3. A specific group of industry experts should be assigned by industry entities to populate each service-specific planning and coordination function.

4. The planning and coordination function should serve as a voluntary industry management resource, acting on behalf of the industry and its regulators.

5. Each group will utilize resources in the industry necessary to complete all of the work activities necessary to accomplish successful service introduction. (See footnote 6).

6. The management activities can be disbanded upon successful service introduction continued in a maintenance mode. National Services must be maintained as such. An example is expansion of 800 Service to include the 888 code (877 and additional expansions in the future will require management and coordination in the same manner as did the initial deployment of 800 Service).

4.2.2.3 National Services Planning and Network Architecture Planning Linkage

National Services planning and Network Architectural planning activities need to be closely coordinated and interactive. Early in the planning process, the necessary architectural resources must be identified. From that, assessments can be made as to the utility of existing architectural assets, in order that effective and timely planning may begin early for enhancements to existing resources or additional resources identified as may be required.

4.2.2.4 Feedback Loops

Both processes that make up the SPPM, the Planning for National Services and the Planning for Proprietary / Regional Services, need to provide information to and feedback from all service providers that are affected on order that they may accomplish the necessary activities and acquisitions in their portions of the network on a known and reasonable schedule.

4.2.2.5 FCC Services Planning Oversight

The FCC should oversee the planning of National Services as recommended in Section 4.7.2 of this report. For the planning of Proprietary / Regional Services, the process will continue to be outside of the Commission's oversight until and unless, formal action occurs to change such services to National Services, with the obvious exception that any Proprietary / Regional Service structure cannot interfere with or defeat the intent of any service that is national in scope. In such cases, the Commission could well take action as necessary to prevent interference, but would still not play an affirmative role in planning the elements of a sub-national service.

4.3 TRANSITION OF ARCHITECTURES, PRODUCTS, AND SERVICES FROM A PROPRIETARY TO A PUBLIC STATUS

4.3.1 Key Learnings

There are three circumstances around which the transition of architectures, products, and services from a proprietary to a public status may be required to take place:

1. Required by mandate of a regulatory body or by national need (*e.g.*, LNP and Universal Service).

2. Market driven which initially or by evolution developed the need for a national standard solution (*e.g.*, ISDN and ATM).

3. Business driven or market driven that are unique and can be applied as proprietary without a requirement for interconnection and interoperability (*e.g.*, Custom Calling Feature List).

In a competitive environment, market forces will drive the development of new products and services. Deregulation is expected to drive technology development and result in shorter service and product cycles which will demand a faster standards development response for interconnection and interoperability requirements.

4.3.2 Recommendations

4.3.2.1 Transition Capabilities

Since market forces will continue to be a key determinate of how and when architectures, products, and services are developed and deployed, proprietary implementations will persist. Therefore, the National Services Planning process needs to address the transition of Proprietary / Regional Services and products to a public status. The *Intermediate Service Realization* in the SPPM represents the transition capability. Service Requirements may be written to include reference to transition procedures that are developed by the telecommunications industry. They should be flexible enough to handle the many transition possibilities and contain industry accepted criteria to promote the expeditious development of the interconnection and interoperability requirements for National Services.

4.4 ACTIVITIES REQUIRED OF EXISTING INDUSTRY FORUMS IN THE PLANNING OF PRODUCTS AND SERVICES AND THE NEED FOR NEW FORUMS

4.4.1 Key Learnings

Industry forums are segmented into two parts: 1) Forums which plan products and services and 2) Forums which plan the architectures which support products and services.

Various activities dealing with the planning of National Services, and their associated Network Architectures (*i.e.,* the "What and How") have proven to be successfully handled by existing Industry forums (*e.g.,* ATM Forum and Carrier Liaison Committee) .

The PTG reviewed the missions of fifty one major industry forums in North America and determined that for national telecommunications products and services there were no committees which were dedicated specifically to the planning or the coordination of planning of such products and services; and for Architecture Forums there was one committee which appears to be relevant to and possibly a venue for various Network Architecture activities as described in Section 4.1 of this report. That committee is the newly formed Network Interconnection / Architecture (NIA) Committee of the ATIS[28] sponsored Carrier Liaison Committee's (CLC) Network Interconnection / Interoperability Forum (NIIF). The mission of the NIA is:

> "The Network Interconnection / Architecture Committee provides an open forum to address and resolve industry-wide technical issues and facilitates the exchange of information associated with telecommunications network architecture and interconnection, including Open Network Architecture (ONA) and/or network interaction."

Functional areas to be addressed by the NIA Committee include:

- Interconnection / Interworking
- Signaling / Switching
- Call Triggers
- Unbundled Elements
- ONA Service Requests
- Notifications (Network Enhancements)
- IN/AIN
- Mediation
- ISDN
- Unbundled Services
- OSS Access
- Protocol

Although National Services and product planning and Network Architecture planning are separate functions and may be pursued by separate forums, their effective development requires that a close relationship exist between their efforts.

[28] ATIS is the Alliance for Telecommunications Industry Solutions that sponsors a number of industry committees in addition to the CLC. These include Standards Committee T1, Telecommunications Industry Forum, Network Reliability Steering Committee, and Internetwork Interoperability Testing Committee.

4.4.2 Recommendations

4.4.2.1 National Services and Products Forum

For National Services and Products, a new Forum should be established as per *Recommendation 4.2.2.2 Participation* and *Activities in Planning for National Services*. Moreover, ATIS, or other telecommunications industry committees or organizations, should develop a proposal, for industry review, for the establishment and management of such a forum.

4.4.2.2 Network Architecture Planning Activities Forum

Network Architecture planning activities as described in *Recommendation 4.1.2.3 Activities Considered Part of Planning Network Architectures*, should be pursued with the newly formed Network Interconnectivity / Architecture (NIA) Committee. To accomplish this, the chair of the NIA should develop a proposal, for industry review, to add the management of Network Architecture Planning activities as an additional functional area to their Committee's responsibility.

Additionally, because of the required close working relationship between both a National Services and Products Forum and a Network Architecture Planning Activities Forum, if the outcome results in two separate forums, there should be a requirement in place that they be managed under a common "umbrella" organization to insure the requisite integration of the individual activities is accomplished.

4.5 IMPACTS OF PROTECTING COMPETITIVELY SENSITIVE INFORMATION ON THE PLANNING AND DESIGN OF PRODUCTS AND SERVICES

4.5.1 Key Learnings

There is a natural tendency for telecommunications service providers and the vendor community to protect their investments in the research and development of products and services. This protection is one of the many responsibilities a company has to its stockholders and its employees and may be manifested by an unwillingness to share information deemed to be proprietary in nature.

If a service and/or architecture is considered to be national in nature, then the following impacts could result if essential information is not shared during the service definition and the architecture development stage in the planning process:

1. Delays in service availability**.** Delays in product and/or services availability would result if technical information vital to the design of interface requirements was not shared.

2. Increased costs for service development. Costs for service development would be higher for the industry if delays and interoperability problems are not minimized during product and/or services development.

3. Interoperability problems during deployment. Interface problems discovered at the time of deployment will delay the introduction of National Services and/or Products and increase the cost to the end user.

4.5.2 Recommendations

4.5.2.1 Proprietary / Regional Services

The position of service providers and vendors to protect competitively sensitive information will continue to be appropriate when dealing with products and services that have not been mandated by the federal government for national availability. The development of proprietary products and services that are not national in scope will continue to be an integral part of the telecommunications landscape. The telecommunications industry should have the freedom to develop innovative products and services so their business can thrive and grow in the telecommunications marketplace. End users benefit from this innovation by having new products and services, industry employees have the challenge to develop these new services, and industry shareholders have the potential to realize their financial goals.

4.5.2.2 National Services (Mandated or Voluntary)

As shown on the Services Planning Process Model (Figure 1), the interaction and sharing of information between telecommunications Service Providers, Vendors, Users, Interest Groups and Regulatory Agencies is necessary for the efficient development of National Services (Mandated or Voluntary) (see 4.2.2.2). The *Requirements Documentation* activity of the SPPM for National Services will specify, along with a number of other outputs, the appropriate interface requirements for the product or service providing each telecommunications service provider and vendor the means to understand the interoperability issues involved. Telecommunication vendors are then able to develop proprietary technical specifications that are required for their equipment. Such vendor-specific implementations may be considered proprietary but can still be capable of meeting interoperability and interconnectivity requirements if there is strict adherence to the national specifications and requirements.

4.6 TIMING ISSUES RELATED TO AVAILABILITY OF NETWORK SERVICES AND PRODUCTS

4.6.1 Key Learnings

Competition within the telecommunications industry could have the unintended consequence of creating vulnerabilities to the service quality and reliability of the nation's telecommunications infrastructure. Minimization of the time it takes to bring new products and features to market can be a powerful competitive advantage that can lead to network incompatibilities and limits on interoperability between networks.

There are a number of consequences that could result from the timing issues between service providers, vendors, standards organizations, equipment vendors, and others.

The Standards Process enhances the level of compatibility and interoperability of telecommunications technology across the industry through consensus and voluntary adoption by the industry of the recommendations. Debates over major issues in attempts to influence recommendations have, at times, caused the Standards Process to take so long as to incite service providers and vendors to deploy pre-standard services and products. Then, first-to-market, as a competitive advantage, drives service providers and vendors to deploy pre-standard services and features prior to the completion of standards recommendations. The fact that balloted standards are voluntary recommendations leaves compliance to standards up to market pressures. Typically, the vendor community responds to the requirements of the network providers, either for services that are standards-compliant or for variations that have not yet completed the Standards Process.

The current and sometimes lengthy cycle of developing voluntary standards by consensus among large industry groups has resulted in some of the following consequences:

1. Vendor pursuit of independent, proprietary solutions.

2. Service provider pursuit of independent, proprietary solutions.

3. Telecommunications industry unable to provide a timely response to market demand.

4. End users incur the cost and inconvenience of having to replace/upgrade equipment.

A service or feature can only be expected to interoperate with the same service or feature in other networks if each is based on a common interpretation of the technical requirements. Once standards are adopted, some interpretation of the technical choices is possible. The chances of different implementations of the same service or feature in different networks is increased when there is a large gap in time when each network deploys the feature.

4.6.2 Recommendations

4.6.2.1 Mitigating the Timing Effects on Interoperability and Reliability

The timing of new service and feature introduction is closely coupled with the issues of regional versus national deployment, proprietary versus public designs, and standards versus non-standards forums. A significant driver determining when a vendor will introduce a new feature or

service into their products and, hence, when service providers can bring those new services to the market is the decision of whether a new service or feature will be standards based or proprietary.

Based on the process flow on the Services Planning Process Model (Figure 1) for National Services (Mandated or Voluntary), architectures, services, and features will be implemented as "standard", not proprietary. The "Open Forum" activities (see 4.1.2.2), including *Standards Developers*, are designed to lessen the impact of a lengthy time interval in producing a requirement, through cooperation and sharing by the industry participants in the process (see 4.2.2.2) and still meet interoperability and interconnectivity requirements.

The process flow for Proprietary / Regional Services recognizes that the development of proprietary products and services that are not national in scope will continue in the telecommunications industry (see 4.5.2.1).

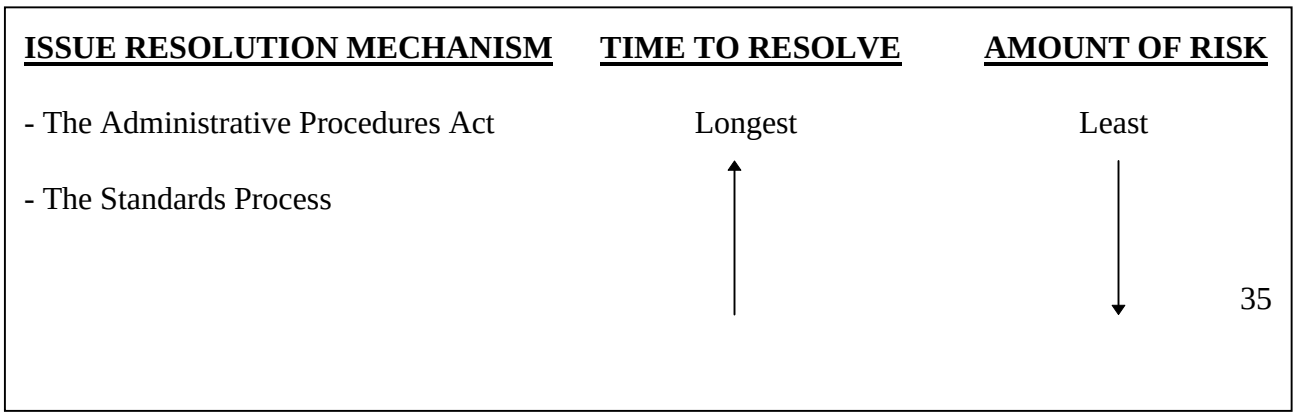
For a more detailed discussion of the standards process and standards developers in telecommunications, see Section 9.

4.7 THE FCC'S ROLE FOR COORDINATED NETWORK PLANNING

4.7.1 Key Learnings

History has demonstrated that industry processes can be used to develop reliable and interoperable network services in a manner that is fast and efficient when they are performed outside of the regulatory arena where policy issues are resolved.

Telecommunications industry participants in the National Services Planning process are looking for some sort of protection against anti-trust litigation as they work the process in order that they can reach consensus on industry issues without concern for legal risks. With regard to the current mechanisms for issue resolution, which include FCC processes under the Administrative Procedures Act (APA), the Standards Process, Consensus Forums and Private Agreements; an inverse relationship often exists between the time required to resolve issues and the associated risks (both legal and technical). That is, issue resolution sought through use of the most lengthy mechanism, the APA, offers the least amount of risk. While issue resolution sought using the quickest mechanism, private agreements, offers the greatest amount of risk (See Figure 2).



- Consensus Forums

- Private Agreements Shortest Greatest

FIGURE 2.

4.7.2 Recommendations

4.7.2.1 Proprietary / Regional Services

The federal government should not be directly involved in the internal development of technical specifications by telecommunications service providers and vendors. Neither should it be directly involved in the development of Proprietary / Regional Services that are not considered national in scope (see 4.2.2.5).

4.7.2.2 National Services (Mandated or Voluntary)

The role of the federal government in monitoring network planning in the telecommunications industry should be that of oversight. The FCC should monitor telecommunications Standards Forums (Accredited & Consensus) activities, as recommended by Focus Group 2, to ensure that interoperability is maintained as a goal during the development of National Services and/or Products. This can be accomplished by advising the FCC of the industry forum activities during the early stages of National Services definition. See Section 9.4.

4.7.2.3 Issue Resolution

The FCC should work cooperatively with the industry processes (*e.g.*, consensus forums, standards bodies, *etc*.) in order to accomplish key interoperability and reliability objectives. The FCC should respond to industry forum requests for action (issue resolution) that emanate from either the *Service Requirements/Definitions* or the *Architectures Goals/Objectives/Concepts* activities of the National Services Planning process and are specific to Section 256 of the Telecommunications Act of 1996, using the most expeditious mechanism available to respond to the industry's needs. A process should be created to allow the industry to escalate such issues directly to the FCC for resolution. The Commission need not take any action, other than their oversight role, unless requested to do so, using the escalation process, by one or more of the industry forums.

5.0 IMPLEMENTATION

The scope of the Implementation Task Group is to evaluate and recommend improvements to the process of deploying networks and services that maximize reliability and minimize interoperability challenges. The focus is on issues that have proved difficult to fully address in the planning process. In addition, our approach has been to develop processes and process improvements to resolve these issues. The analysis looks at the following: 1) today's interconnection environment; 2) review and modification/enhancement of the existing Network Reliability Council's (NRC II) Network Interconnection Bilateral Agreement Template and Network Interface Specification Template; 3) information sharing; and 4) industry liaison processes.

5.1 TODAY'S INTERCONNECTION ENVIRONMENT

5.1.1 Key Learnings

On July 6, 1994, Reed Hundt, Federal Communications Commission (FCC) Chairman, stated in his introductory remarks before the NRC II "we are here to address questions about network reliability in an era when technological change is proceeding at a blinding pace, and markets are evolving in ways not anticipated even a few years ago."

In executing its mission to "evaluate and recommend improvements to the process of deploying networks and services that maximize reliability and minimize interoperability challenges," the Implementation Task Group believes that as a prerequisite, today's interconnection environment must be fully defined and understood. In that context, the team will address these key issues:

- NRC II Network Interconnection Bilateral Agreement Template and Network Interface Specification Template
- Information Sharing
- Industry Liaison Processes

Today's interconnection environment must be reviewed from both perspectives identified in Chairman Hundt's comments -- technology forces and market/public policy forces. In the background section of its recommendations, the NRC II Increased Interconnection Focus Group 2 noted that " several driving forces are at the root of this study effort: deregulation, competition, and technology changes."

While the recommendations made by the NRC II appear to be based on these forces, they were predicated on the 1994-1995 time frame. It is the intent of this task group to review those recommendations in the context of implementing increased interconnection and interoperability triggered by the passage of the Telecommunications Act of 1996 and, with the objective of

addressing implementation issues, update them based on technological, market, and public policy environmental changes that have occurred since the NRC II work.

Market/Public Policy Environment

Prior to the 1980's, the pace of change was driven more by technology and market forces than by public policy change, particularly in the public telephone network. During the 1980's, the industry did not think in terms of interconnecting networks but rather in terms of equal access to existing networks. As a result, "interconnection" was generally managed by standards development activities, recommended practices, equipment compatibility, *etc.* as a part of an overall evolutionary process.

Coincident with the FCC Computer Inquiry proceedings in the early 1980's, deregulation of customer premises equipment and the divestiture of the Bell Operating system, the pace of interconnection change began to accelerate as a result of public policy as well as technology. However, because there was sufficient lag time between events, the industry had time to keep pace. Further, each of these events created new and unique points of interconnection within a previously homogeneous public telephone network. These events not only resulted in the creation of new points of interconnection but a multiplicity of service providers seeking to enter the new markets that resulted. The industry also responded by creating new processes and organizational structures such as the Alliance for Telecommunications Industry Solutions (ATIS). (See Section 4, note 28.)

During the 1980's, the fact that the new providers were largely from the wireline segment was due, in part, to attempts by public policy makers and providers to separate markets by technology and by the nature of the services provided. As a result, interconnection between local exchange carriers and other providers did not occur as often as it might have otherwise. By the early 1990's, it became apparent to the policy makers that such attempts could not be sustained because the competitive and technology forces were too great.

The FCC recognized that the reliability issues addressed in NRC I represented the traditional public switched network. The Commission assembled the NRC II in January, 1994, recognizing the environment was rapidly changing to a multi-provider, multi-vendor paradigm. Consequently, the Commission took pro-active steps to see that the industry established and shared recommended best practices to ensure the reliability of the public telephone network in the new "network of networks" era.

Since NRC II, the pace of public policy change has accelerated as never before with the passage of the Telecommunications Act of 1996 and other policy-related activities such as spectrum allocation and personal communications systems (PCS) licensing. When combined with the accelerated pace of technology change, this new interconnection environment is challenging the industry as never before.

The Telecommunications Act of 1996 established, among other things, requirements for interconnection between providers of local exchange service; access to unbundled network

elements of incumbent local exchange providers; and resale of incumbent local exchange provider services. Each of these requirements results in a significant increase in the number of providers of local exchange services, potential number of points of interconnection, and the operational and administrative needs of the interconnectors. This expands the scope and raises the stakes for service providers to engage in greater coordination efforts for increased interoperability .

Given the Congressional mandate for federally guided state involvement and bilateral, negotiated interconnection, diverse interconnection scenarios are emerging. And while the unbundling of network elements will initially be based on technology that was designed to be integrated, technologists will likely respond to the unbundling requirements with more efficient designs.

Technical Environment

Historically, there were few reliability and interoperability problems due to the fact that a single entity designed, built, installed, and operated telephone equipment and service. A major factor of the historical success was that there were defined standards and little choice but to implement them. Competition has changed all of that.

With competition, an effort has been made to maintain standardization in a multiple-provider, multi-vendor environment. This is accomplished through various domestic and international standards bodies and industry forums.

However, with this approach, there are possibilities that standards may be insufficient or "subject to interpretation". This missing information may ultimately result in the inability of different parties to interconnect and interoperate without significant additional work. These interoperability challenges extend from the physical layer to the application layer of the Open Systems Interconnection (OSI) model. Currently, these gray areas are being resolved through significant iterative efforts in planning and testing.

Impacts

Several factors significantly increase the difficulty of achieving seamless interoperability as networks are implemented. While any one factor by itself poses no serious challenge, the collective influence of several factors and all of their permutations create a serious impediment to simple interoperability. Some of the major factors are briefly described below in random order.

- Technological rate of change -- In the past there was a "best" way to do things. This "best" practice was developed after a lengthy analysis and evaluation. In today's environment, the number of different technological options is continually growing. Concurrently, the time between idea and implementation has been significantly reduced. There is often not enough time for the industry to develop guidelines before those guidelines are already obsolete. Even when a standard is agreed upon, there is the issue of timing. Sometimes the standard exists in advance of the implementation. While certainly more convenient, pre-implementation standardization does not ensure interoperability. The more likely situation in

today's environment is that the standard may sometimes lag the actual deployment time frame. In this case, the actual deployment faces the dilemma of continued non-compliance or costly conversion to standards. Even if the desire is for standards compliance, the conversion may negatively impact existing customers' service. Business decisions and market factors will drive the final technology decision. Companies must make decisions that are sometimes in conflict with standards development and market timing[29]. For example, when the Asynchronous Transfer Mode (ATM) standard was being developed, efforts were initially focused on Synchronous Optical Network (SONET) Optical Carrier Level-3 (OC-3) and OC-12 physical interfaces. Since SONET deployment was progressing more slowly than anticipated, many vendors developed ATM over DS-3. With DS-3 ATM being widely deployed, the ATM Forum re-addressed the issue and developed the official ATM over DS-3 standard. Recommendations to improve the standards process are discussed in Section 9.

- Rate of implementation -- Even if a comprehensive standard exists, there are many non-technical business factors that result in widely varying rates of implementation. In some cases, an end-to-end standard exists but its usefulness is thwarted by a lack of consistent deployment. In other cases, a carrier may choose to never deploy a technology for either offensive or defensive competitive reasons.

- Different operational requirements -- Just because a standard exists does not guarantee that it will be implemented in the real world. A current example would be the optical mid-span meet. While it could be done technically, it creates difficulties for real time network management. Challenges such as fault isolation, point of demarcation, trouble notification, repair coordination limit the usefulness of the implementation. Some carriers may avoid this arrangement for business reasons even though it may be a technically superior solution.

- Different key service requirements -- Providing an end-to-end service requires that many different levels of interconnection and interoperability be addressed. Even though data can now pass from end to end, there may still be operational differences in the service. One carrier may believe that service availability is the most critical parameter, while another may believe that error free performance is the most important. This can create confusion when one network reports a problem in another network while that network is operating as expected. It also underscores the need for negotiation and mutual cooperation between service providers who are often competitors.[30]

- Different business drivers -- A goal of many networks is interoperability. However, in an attempt to add value or remain competitive, owners of a network may choose to implement an interface that is non-standard. Where strategies conflict, a tremendous challenge to interconnection results.

[29] Section 4.6.2.1 (Interoperability Planning) contains a recommendation for mitigating the timing effects on interoperability and reliability.

[30] Operational performance issues are addressed in Section 6.0 (Operations).

While this may be a real but infrequent situation, one service provider could choose a set of standards options that best fits its business needs, requiring other networks to adopt the same options or implement more costly alternatives. All of this can occur with a "standard" interface. There may also be situations where implementing a standard would negatively impact the business. While some network service providers may say they want interoperability, they will adhere to the standard in their implementation only if it meets their business needs.

Other business concerns such as information security or company image may drive sub-optimized interconnections. An example might be where a competitive access provider (CAP) carries traffic for competing interexchange carriers (IXC). Cases exist where CAPs were not permitted to pass one interexchange provider's traffic through another IXC's site. To meet the needs of both customers, the CAP may be pushed to implement a more costly solution.

It is a frequent occurrence that competing carriers provide mutual aid capacity to help a competitor deal with a network outage. While this is done today at the well standardized DS-3 level, this will become more difficult as carriers transition to SONET due to the added complexity of the SONET overhead.

- Next generation network -- A carrier's future network evolution plans directly influence implementation decisions made today. Questions which affect the level of interoperability that is possible today include:

  - Should the core network be time division multiplexed (TDM), ATM or internet protocol (IP);
  - Should the survivability mechanism be SONET or ATM.

  While the carrier's future network may offer the ultimate in interoperability, the path to get there may cause delays to other providers.

- Computer versus telephone -- While most telecommunications equipment relies heavily on computers and most computers rely heavily on telecommunications services, each sector drives common problems to a different set of solutions. The computer industry has invented new high speed interfaces that are convenient to implement in the computer network. Telecommunications providers have invented new high speed interfaces that are convenient to interwork with existing systems. Although this has created a market for solutions to interconnect the two factions, the added complexity has challenged efficiency and interoperability.

Challenges

Even though there are many business factors influencing interoperability, there are also many technical factors. Many of these are under the direct control of the industry. Some of the major factors are described below in random order.[31]

- Standard options - One of the challenges a carrier or vendor must face is which standards to follow in the implementation. Standards are developed in several organizations, including the International Telecommunication Union (ITU), the accredited committees and organizations of the American National Standards Institute (ANSI) and industry forums. All may be developing somewhat different standards addressing a common issue. Even when a single standard is developed, it may provide various options within its bounds, thereby creating an environment where there are number of choices to be made.

  Selection of one set of options can result in incompatibility with other options. As a result, industry forums, such as the ATM Forum and the SONET Interoperability Forum, have been created to develop implementation specifications.

- Areas not addressed by standards - A single standard may not address all aspects of a technology implementation. A standard is a product of its standards body's charter and rules for consensus. In some cases, additional work must be done to actually implement the standard.

- "Standard" gray areas - There are also areas of standards that either don't define enough or define something in a way that is subject to interpretation. Usually the standard is perfectly clear to those that participated in its creation. However, others not involved in the process must take the standard at face value. In some cases, the gray area exists due to the inability to reach consensus on a particular aspect of a standard.

- Interim solutions - Related to standards timing is the issue of deployment. In an effort to be first to market, an interim solution is frequently implemented. This interim solution may be based on a best guess of where the standard is headed or it may be based on ease of implementation. In either case, the interim solution must eventually be migrated to the final standard or continually "worked-around."

- Multiple levels of interoperability - As technology progresses, new levels of interoperability are required. For an over simplified example, what should the physical media be? Air, copper, fiber? If air, what frequency and modulation scheme? If copper, what type? If fiber, multi-mode, single-mode, dispersion shifted, non-zero dispersion shifted, dispersion compensating? Continuing with the fiber example; what wavelength of laser? What modulation scheme? What power?

---

[31] It should be noted that this discussion is key to understanding today's interconnection environment. This tension between market needs and the desire for standardization is addressed in Section 4.0 (Interoperability Planning) and Section 9 (Standards Development Process).

The paragraph above only deals with physical connection. Is the fiber transport Plesiochronous Digital Hierarchy (PDH) or SONET? What rate? What protection scheme? What multiplexing structure? What synchronization hierarchy? Data Communications Control Channel (DCC) protocol? What DCC messages?

Once the above decisions have been made, there is only a network connection available to transport information. Is there an intermediate transport protocol such as ATM or frame relay? How is signaling handled? What is the application? Voice, video, data? Is it domestic or international? How is the service provisioned, billed, supported? At every level in the previous example there is the opportunity to select incompatible options. Careful consideration and joint planning are keys to ensure compatibility at all levels of interoperability.

- Administrative systems (Back office systems) - Related to the multiple levels of interoperability, the issue of non-real time support systems is frequently dealt with after all of the real time network issues are resolved. While the service may be available, the coordination between carriers' support systems may not have been fully addressed. This may involve how the end-to-end service is provisioned and billed; and how customer service and service difficulties are addressed. Without considering the total process, full interoperability has not been achieved.

- Business choice / equipment limitations - Even in an environment where there is strict adherence to standards, there may be equipment limitations that prevent a desired level of interoperability. An example might be that one carrier wants all SONET OC-3 interfaces to be protected on a one-for-one basis. The connecting carrier's equipment may not be capable of supporting that requirement. Due to the large number of options within a single standard, it may be impossible or not cost effective for an equipment manufacturer to implement them all.

- Proprietary solutions - Additional interoperability requirements brought about by competition created a greater need for standards. At the same time, a competitor may want to differentiate or add value with a proprietary implementation. If everything is completely standardized, services would become a commodity. The challenge is how to differentiate a service while maintaining technical compatibility with the rest of the industry. Frequently this is accomplished by implementing proprietary solutions within a network while presenting a "standard" interface to other networks.

- Not invented here - There is also the situation where company expectations drive technology implementations. It might have been a superior implementation that did not survive the standards creation process. It might also be a business driven solution.

- Legacy systems - One of the biggest challenges any carrier faces is the migration to new and better networks and operational support systems. Issues such as quality of service may make the transition difficult. Economic factors also control the rate of migration. In reality, there

will always be legacy systems that will create an interoperability challenge. In addition, the trend is toward distributed systems creating more opportunities for interworking.

5.1.2 Recommendation:

Due to the Telecommunications Act of 1996, the pace of public policy and technology-driven changes surrounding interconnection has accelerated significantly. Further, this increased pace of change is occurring at an increased number of venues (*i.e.,* state activities). It is during this period of time that concerns for interoperability are greatest. The various industry segments should organize themselves to ensure that risks to interoperability are minimized through such means as increased information sharing and improved liaison processes. While there are no specific recommendations by the Implementation Task Group which come from this discussion, it is important to understand that it is in this context of today's interconnection environment which the task group evaluated these key issues.[32] While standards development processes may be stressed by many factors, as described above, the processes are still viewed as an effective means of improving interoperability. The recommendations in Section 9 are designed to enhance the standards process.

5.2 REVIEW AND MODIFICATION/ENHANCEMENT OF NRC II TEMPLATES

5.2.1 Key Learnings

In 1996, NRC II issued two templates to serve as tools for facilitating the technical aspects of interconnection agreements between network providers. These templates, namely the Network Interconnection Bilateral Agreement Template and the Network Interface Specification Template, were then distributed throughout the industry as part of a compendium of technical papers entitled Network Reliability: The Path Forward.

The Implementation Task Group took as one of its initial tasks the review of these templates and the determination of how effectively they were being used for the development of existing interconnection agreements. Due to the templates focus upon the standards development process (not the bilateral agreement development process), the Implementation Task Group has not modified the Network Interface Specification Template. Instead, the NRIC's Focus Group 2 has made some changes and recommendations that are further explained in Section 9.2.

Samples of interconnection agreements were examined and found to be general in nature, reflecting legal as well as pricing terms and conditions with a high level look at some of the topics detailed in the templates. In most cases, types of services to be interconnected, interface specifications, plus forecasting, installation, provisioning, and maintenance guidelines and

[32] While there are no specific recommendations which come from the Implementation Task Group, recommendations addressing many of the issues discussed in this section are contained in Section 4.0 (Interoperability Planning), Section 6.0 (Operations), and Section 9.0 (Standards Development Process).

responsibilities were described in general terms. However, many topics within the templates were not covered. Based on the contents of agreement samples and discussions with various personnel involved, negotiators did not appear to be fully utilizing the templates as a tool; and some were not aware of them at all. The Implementation Task Group found that the level of detail specified in the templates was simply not explicit in most of the existing interconnection agreements that were examined. However, the Task Group did determine that the NRC II Network Interconnection Bilateral Agreement Template in particular, may be useful to those who are currently negotiating technical agreements, at least as a checklist of issues that may be discussed in the course of technical/operational negotiations.

Based on this study, there appears to be at least two steps to the process of negotiating interconnection agreements. The first step identifies the legal, pricing, and general operational parameters negotiated between the interconnecting companies. At the time of the study, this step was covered by most of the existing interconnection agreements. A second step includes a bilateral agreement(s), addressing the technical aspects of interconnection as well as particular operational guidelines, such as performance measurements. These are the agreements that are, in most cases, currently under development, as depicted in Figure A.

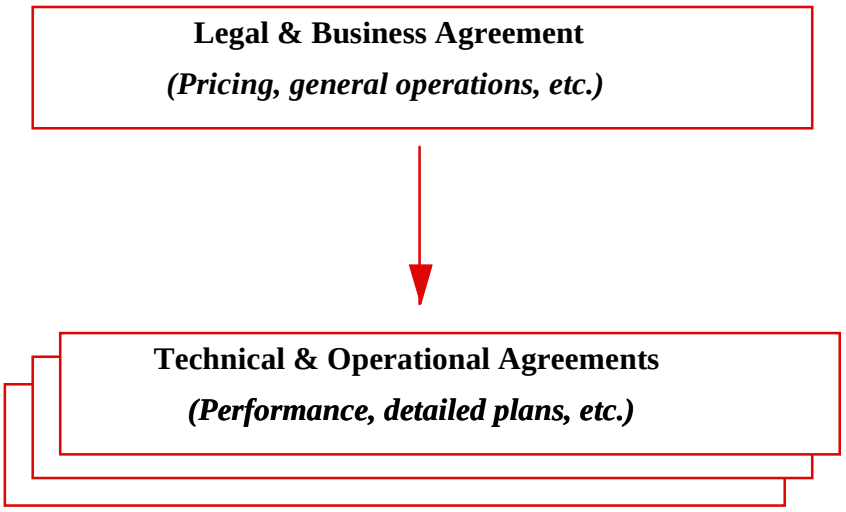


Figure A: Interconnection Agreement Steps

5.2.2 Recommendations

5.2.2.1 Re-Distribution of the NRC II Templates

Because of the breadth and scope of the NRC II compendium, the templates may not have found their way to the personnel involved in current interconnection agreement negotiations. After an initial review of the templates, the Implementation Task Group felt that an immediate re-dissemination of the original templates was timely as many companies were already engaged in negotiations. In addition, re-dissemination would serve as a vehicle for soliciting input and suggestions on further template work.

Re-dissemination targeted working-level personnel in interconnecting companies, rather than relying on information to trickle down from higher level recipients. Lists of target personnel were developed from a variety of sources in an effort to make the list as comprehensive as possible. The NRC II templates were re-distributed with an explanatory cover letter in January, 1997. Appendix A contains the cover letter and the list of recipients.

5.2.2.2 Modification/Enhancement of the Network Interconnection Bilateral Agreement Template

The Implementation Task Group reviewed the templates in light of the experience gained by participants in local interconnection negotiations as well as in the implementation of the Telecommunications Act of 1996. Most of the changes to the Network Interconnection Bilateral Agreement Template reflect the reorganization of sections based on functionality, the clarification of the purpose of these sections, and the addition of relevant topics to these sections. For instance, details relating to issues such as resale, unbundling, network security, and billing have been added. While the Network Interconnection Bilateral Agreement Template may not encompass all issues involved in negotiating every agreement, it is designed to serve as a checklist for highlighting issues that may be addressed in the course of negotiating technical/operations interconnection agreements or amendments. The complete Bilateral Template can be found in Appendix B. Within the body of the template, items that are asterisked (*) may pertain to unbundling and/or resale. However, these may not be the only items pertaining to these issues.

The following sections, 1.0 - 7.0, describe the new organization of topics within the Network Interconnection Bilateral Agreement Template:

1.0 Requirements and Agreements for Provisioning Network Interconnection

This section identifies the preliminary parameters on which the technical/operational bilateral agreement is built. Reaching a clear understanding on such topics as network design parameters and service level expectations forms the foundation vital for the success of further agreement development. In addition, discussion of electronic bonding requirements and various parameters for SS7 interconnection are vital. Therefore, agreements on service levels is one likely outcome of this phase of interconnection negotiation.

2.0 Installation and Maintenance Guidelines, Procedures, and Responsibilities

This section details the guidelines, procedures, and responsibilities for installing and maintaining network interconnection. Therefore, contact lists for Inter-Network Trouble Resolution and Escalation Procedures, Emergency Communications Plans, and Mutual Aid Agreements may be important results of this phase, as is the establishment of performance levels associated with installation issues.

3.0 Interconnection Testing Procedures and Responsibilities

This segment specifies the procedures for testing the performance of various types of network interconnection, including network and SS7 testing. Various existing testing procedures should be referenced for both pre-cutover and post-service testing and reporting. Therefore, details regarding various test plans as well as contact lists for these plans may be critical outputs of this phase of a bilateral agreement.

4.0 Network Administration and Management Guidelines, Procedures, and Responsibilities

This part of the agreement describes network administration and management procedures and responsibilities within the bilateral agreement. Therefore, documentation regarding network configurations and reconfigurations for such issues as security, load considerations, network management and synchronization, as well as associated contact lists, are suggested results from this area of agreement development.

5.0 Network Transition Considerations

This section specifies considerations for planning for interconnection as the networks evolve and emerging technologies are introduced. As a result, network transition plans and procedures for the interconnection of new technologies as well as the retirement/removal of old equipment may comprise the tangible outputs from this phase of the agreement.

6.0 Billing Considerations

This portion examines aspects of network interconnection that affect expedient and proper billing. Efforts in this phase may produce appropriate billing methods and procedures that ensure accuracy and timeliness as well as the procedures for exchanging billing records.

7.0 Vendor Requirements and Responsibilities

This section of the bilateral agreement examines the requirements and responsibilities associated with the vendors and manufacturers of the elements to be interconnected. Resulting products from this aspect of negotiation may include contact lists, emergency procedures, and agreements for vendor-provided training and testing. Vendor roles in training and testing may be particularly important for emerging technologies.

The following topics and explanations describe major additions the Implementation Task Group made to the Network Interconnection Bilateral Agreement Template.[33]

[33] This section references many committees that are sponsored by ATIS. See Attachment C for an ATIS organization chart, directory, and contact information.

- Audit Requirements - This item has been included as a security consideration when negotiating interconnection.[34] When provisioning new services, information such as who requested action, who took action, and when that action was taken, may need to be tracked.

- Access Control and Authentication Requirements - This item has been included as a security consideration when negotiating interconnection. For example, procedures are being developed to appropriately authenticate, secure, and limit access. The Electronic Communications Implementation Committee's (ECIC) Security Committee, a committee of the Telecommunications Industry Forum (TCIF) sponsored by ATIS, addresses encryption and security options for information exchanges between different systems from an operations, administration, maintenance and provisioning (OAM&P) perspective.

- Compatibility of Expanded Use of Information Digits - The expanded use of information digits will continue as service offerings and system capabilities grow. In an interconnected environment, compatibility in the application and transporting of these digits, where available, is important for enhanced services and systems to be workable in an interconnected environment. The Network Interconnection Interoperability Forum (NIIF), sponsored by ATIS, is currently working on this issue.

- Directory Listings - Guidelines on the exchange of directory listing information between interconnectors are needed for a variety of scenarios. For instance, a provider may list another provider's customers in its own directories. Similarly, a provider may furnish a complete set of its listings to the other provider for use in that provider's network. In these cases, identifying parameters such as the media for exchange and the data format is essential. The ATIS Ordering and Billing Forum (OBF) Ad Hoc Directory Committee is examining issues associated with access to directory assistance and modifying current processes to accommodate new local service providers.

- Electronic Bonding - To support resale and unbundled ordering and provisioning of services in an interconnected environment, the FCC has ordered non-discriminatory access to the incumbent local exchange carriers' (ILEC) operations support systems (OSS). Electronic bonding allows the reseller to access the ILEC's OSS on a real-time, on-line basis. To ensure proper functioning of electronic bonding on a given OSS interface, interconnectors must agree on various technical specifications, such as message sets exchanged, availability, and throughput. Currently, there are a number of subcommittees involved in this effort. For example, specifications for electronic bonding are being addressed in the TCIF's Electronic Data Interchange Committee (EDI Committee). In addition, the Operations Task Group of Focus Group 1 has defined the functional requirements for an electronic gateway. (See Section 6.)

- E911 Database Updates Agreements and Guidelines - Due to the importance of the E911 database, agreement on E911 parameters has been singled out for particular attention during

[34] The addition of security related elements to the template were made at the request of Focus Group 1's Operations Task Group. (See Section 6.)

negotiations. For example, parties must agree on how often the E911 database will be updated. Then, identifying E911 guidelines and procedures, such as how the database updates will be performed, is crucial for negotiations. The NIIF is currently working on this issue.

- Firewall Administration and Management - This item has been included as a security consideration when negotiating interconnection. Examples of parameters to negotiate include identifying what information is allowed to pass between networks and/or users and what information is to be restricted.

- Local Number Portability (LNP) - LNP has been included in the checklist as a service requiring appropriate guideline agreement. LNP is actually divided into two categories, namely interim LNP and long-term LNP. Each category has its own issues. Interim LNP is based on switching functionality. A number of variations on interim LNP are available, each impacting services and operations in different ways. Some interim LNP implementation methods include Remote Call Forwarding (RCF) or Direct Inward Dialing (DID) method.

  Long-term LNP is based on queries to LNP Service Control Points (SCP), which will provide the routing information for the ported number. Various committees both on a state and national level are establishing processes for porting numbers, testing, and administering Local Routing Numbers (LRN). These committees are identifying requirements for updating LNP databases.

  Further, number portability issues are being investigated in several venues such as the ATIS-sponsored T1S1 Technical Subcommittee (Services, Architectures and Signaling), the Industry Numbering Committee (INC), and the FCC's North American Numbering Council (NANC). The NIIF is currently working on LNP in several of its subtending forums. The Network Management Committee (NMC) is developing an LNP Test Plan, NIIF Issue #0024, in cooperation with the NIIF Network Installation and Maintenance Committee (NIMC). This issue will develop an industry test plan for long term service provider portability as mandated by the FCC Order in CC Docket No. 95-116. The NMC is working with the Illinois Number Portability Workshop and their "Local Number Portability LRN Test Plan."

  The Network Rating and Routing Information Committee (NRRIC) of the NIIF is working NIIF Issue #0036, "Local Number Portability Routing Requirements". This issue will identify the Traffic Routing Administration (TRA) documents that must be modified to support LNP. The NRRIC has provided the industry input (*i.e.,* requirements data) to TRA so that the Local Exchange Routing Guide (LERG) system modifications work to accommodate LRN can begin. Clearly, consideration of both interim and long-term LNP requirements is important for achieving interconnection.

  The Network Testing Committee (NTC) of the NIIF is developing an LNP Test Plan to test the internetwork interconnection aspects of LNP. The NTC is developing the tests scripts and has a preliminary test schedule.

- Main Distribution Frame (MDF) Requirements - This addition stems from the Telecommunications Act of 1996 mandate requiring ILECs to provide access to unbundled loops. For these unbundled loops, the point of interconnection will occur at the MDF (or an equivalent point which may be determined during negotiations).

- National Services (Toll Free Services, 500 Services, 900 Services, Line Information Data Base-LIDB) - Development of guidelines for national services is important. Guidelines would include access to numbers, the updating of databases, *etc.* Currently, there are a number of committees involved in this effort. For example, the OBF Service Management 800 Number Administration Committee (SNAC) is addressing issues associated with toll free services. In addition, the ATIS NIIF Network Rating and Routing Information Committee (NRRIC) has responsibility for issues associated with LIDB.

- OSS Interface Requirements[35] - Interconnectors, particularly resellers and unbundled element users, may need information from wholesalers regarding operations support systems (OSS) as they may need to send data to and receive data from these OSS. If this is the case, agreements on access methodology, security requirements, time frames, types of data exchanged, and performance criteria are important. When direct access is not allowed or required, access to necessary information may occur via a gateway OSS. This issue is closely linked to the Electronic Bonding Issue described earlier, and the functional criteria discussed in Section 6.

- Process for Circuit Level Testing and Performance Analysis of Unbundled Elements - Access to unbundled elements means that elements from several networks may be used when establishing a single end-to-end service. The ability to evaluate and test this type of service needs to be assessed.

- Process For Certifying Operation of Combined/Intermingled Network Elements - Vendors may also have responsibilities within technical/operational interconnection agreements based on their product capabilities. Interconnectors may desire additional vendor support in achieving proper interconnection, especially with regard to emerging technologies. Examples of this support may include how to properly test a network element and how can it be managed once the network is in place.

- Resale Related Service Requirements (Network) - This addition arises from the FCC order related to operator services/directory assistance (OS/DA) routing and branding. This creates a need for processes that allow a reseller to choose and change how OS/DA calls will be handled for their customers. Therefore, resale related service requirements may entail consideration during negotiations.

- Root Cause Analysis Processes - It may be helpful for interconnectors to concur on specific processes for jointly performing root cause analysis. This information should also be included in an agreement.

---

[35] OSS Interface issues are addressed in Section 6.0 (Operations).

- Security Testing and Auditing Procedures - This item has been included as a security consideration when negotiating interconnection. For instance, defining a process for proactively testing networks to determine system weaknesses to ensure security measures are working properly is important.

- Service Provisioning Process - With this addition, the checklist now contains further detail regarding provisioning interfaces. Resellers and unbundled element users must be able to order services in a smooth and convenient manner. Therefore, agreement for criteria such as timing intervals and error handling is vital for reliable interconnection. The NIIF is currently working on this issue.

- Services Related Operational Guidelines - Due to the prominence of services such as national services, directory listings and number portability, this category has been added to the checklist for completeness. The NIIF is currently working on this issue.

- Special Routing Translations (SSP, STP) - Where and when allowed or required, special routing translations must be identified and arranged in the course of negotiations.

- Specific Versions of Protocol - As a generic requirement for any interface with multiple versions and options, interconnectors need to agree on definitions of what is optional and what is mandatory. Agreement must be reached on such issues as what to do with optional parameters, how much backward compatibility will be supported, and how to plan compatible migrations.

- Transition of Use of Emerging and Future Technologies - Standards for emerging technologies are continually under development. In cases where there are many versions and options involved, interconnectors may need to invest additional effort in ensuring compatibility, particularly for feature interactions. Discussion should also occur when network elements are updated or replaced.

- Unbundling Related Services Requirements (Network) - This addition arises from Telecommunications Act of 1996 mandates regarding access to unbundled elements. Both the users and owners of unbundled elements must reach a mutual understanding of requirements and capabilities of each element. Defining the process to be followed if the user wants to provide ISDN on an unbundled loop is one requirement example. Another involves certain translations. In this example, dialing plans may be specific to a user of a particular unbundled element. Clearly, agreeing on these requirements is necessary for successful interconnection.

- Year 2000 Compatibility - By design, many computer systems represent calendar dates in six digit format (*e.g.,* YYMMDD). Unfortunately, this format will cause problems as the end of the twentieth century draws near. As a result, many systems are being updated to accommodate the new format required for successful operation in the twenty-first century. Because date information must be exchanged between service providers in routine processes

such as provisioning flows, interconnectors must ensure that their year 2000 conversion efforts are compatible.

5.2.2.3 Publishing of the Modified/Enhanced Network Interconnection Bilateral Agreement Template

While the revised Network Interconnection Bilateral Agreement Template may not encompass all issues involved in negotiating every agreement, it is designed to serve as a checklist for highlighting issues that may be addressed in the course of negotiating technical/operations interconnection agreements or amendments. Therefore, the Implementation Task Group recommends that it disseminate the revised Network Interconnection Bilateral Agreement Template under separate cover to those working level personnel targeted for the NRC II template(s) re-distribution effort detailed in Recommendation I of section 5.2.

5.2.2.4 Suggestions for Effective Use

Depending upon the wishes of the negotiating parties, the Bilateral Template may be used either as one complete unit or as a means to address particular issues individually. For example, addressing issues individually may ensure that key points regarding that issue are not overlooked. Examples of these types of issues include network interconnection, unbundling, and resale. This method may be helpful as perspectives may change depending upon the issue under consideration. Furthermore, in order for the Bilateral Template to remain a viable tool, future revisions may be necessary. As other emerging issues become more well defined, future additions and revisions will be required.

5.2.2.5 Template Custodian

The recommended custodian of the Bilateral Template is the Network Interconnection and Interoperability Forum (NIIF), sponsored by ATIS. This newly organized forum merges the work and activities of the former Network Operations Forum (NOF), the Industry Carriers Compatibility Forum (ICCF), and the Information Industry Liaison Committee (IILC). Its mission is to provide an open forum to encourage the discussion and resolution, on a voluntary basis, of industry-wide issues associated with telecommunications network interconnection and interoperability. This includes network architecture, management, testing, and operations. The NIIF is recommended to regularly review the Network Interconnection Bilateral Agreement Template and amend it as necessary. The Implementation Task Group further recommends that the NIIF establish processes (or use existing processes) to facilitate the review and update of this template. These processes should include, at a minimum, that template users, whether or not they are NIIF participants, are able to submit suggestions for changes/additions by contacting the NIIF Director resident at ATIS. The importance of having user-friendly processes to update the Network Interconnection Bilateral Agreement Template is emphasized.

Though the NIIF is the overall custodian, certain template issues are the responsibility of other organizations. For example, billing issues are the responsibility of the OBF. Therefore questions concerning issues outside of the NIIF area of responsibility should be directed to the appropriate

organizations by the NIIF.

5.3 INDUSTRY LIAISON: IMPROVED PROCESSES

The Implementation Task Group examined the need for improved liaison processes from two perspectives: 1) Whether a centralized liaison process should be the vehicle by which to achieve the long term sharing of information associated with network interconnection and implementation; and 2) what industry liaison processes are needed specific to the enhancement and ongoing maintenance of the Network Interconnection Bilateral Agreement Template.

5.3.1 Key Learnings

General Liaison Processes

The scope of the Implementation Task Group's activity was to evaluate and recommend improvements to the process of deploying networks and services that maximize reliability and minimize interoperability challenges. In generally discussing the needed improvements by the industry in deploying networks and services in the current environment, the Task Force identified a missing link - an effective and efficient centralized industry liaison process. The Task Group recognized that in many instances, liaison processes between the telecommunications industry and representative organizations (*e.g.,* trade associations/organizations which represent their respective industry segments) existed. It was also recognized that numerous organizations, committees, and forums addressing telecommunication issues have liaison mechanisms internal to their processes. Furthermore, where an industry need may have prompted a liaison between industry segments or organizations, the liaisons were established to fill an immediate and often temporary need for information sharing. In some cases, the "temporary" liaisons may have duplicated existing work efforts or overlooked issues that were already addressed elsewhere. Thus, it appeared that there was no centralized process to facilitate these important exchanges of information or to better publish what has already been done within the industry and by the industry.

The Task Group also considered whether liaisons as information sharing tools are effective and thus, continue to exist as they do today (*i.e.,* primarily internal to organizations or industry segments) or whether a more formalized, "centralized liaison process" would better serve the needs of this dynamic industry. Thus, the Task Group thought a closer look at the prospect of a centralized liaison process was warranted.

There is much to take into account in establishing a liaison process. Some of the immediate issues raised by the prospect of such a process are: What is a liaison? Why is a liaison needed and what should its objective be? How should the liaison process be used? Who is the universe of participants (*e.g.,* industry forums, organizations, specific industry segments) that should participate in the liaison processes? How might this liaison process be managed? How would the process's effectiveness be measured?

Initially, the Task Group thought that the more formalized/centralized liaison process warranted consideration. It seemed to address a missing need for a greater understanding by more industry players as to where to get information, who was working on key issues related to interconnection, and who may have had an experience in implementing the technical/operational aspects of interconnection agreements and addressed some matter worth sharing with others in the industry. It appeared that even within those companies and organizations represented on the Task Force, there was a wide array of sources for such information that simply needed a centralized way to be shared.

Moreover, it was thought that two concerns could be addressed by a centralized liaison process: 1) it could be responsive to smaller companies who do not have the opportunity to attend industry meetings on a regular basis; 2) it could make information more accessible on all industry activities which might be addressing a particular issue such as network testing. The Task Force recognized that even for the more seasoned participants in the industry activities, there are so many different groups, sponsored by both organizations and industry segments, which have valuable activities. And, because of their numbers, it is difficult to know all of the opportunities to access such information.

As a result of this understanding of the problem, the Task Force undertook trying to develop a centralized liaison process and some superstructure by which liaisons could occur and be managed. In accepting this approach at the outset, it appeared that a starting place was to identify those industry forums, committees, organizations and their respective members/participants which might participate in a centralized industry-wide liaison process. At a minimum these information sources identify those players which might benefit from increased communications within the industry and knowledge of each others existence as sources of information on interconnection.

The Task Group examined the centralized liaison process. Recognizing the challenges of the centralized liaison, including establishing some superstructure who might manage it, as well as fund and staff it, the idea seemed to have more hurdles and costs than overriding benefits. Moreover, it was recognized that the industry is moving towards greater efficiencies and less structure. As such, it was concluded that the better approach would be to centralize the sources of available information, rather than centralize the liaison process.

5.3.1.1 Establishment of a Homepage

In order to centralize sources of available information, the Task Group recommends the establishment of a homepage as a billboard and as a single source for activities and issues related to the implementation of interconnection. Such a site could also then serve as the catalyst for liaisons. If users of the site find valuable information on an important interconnection issue to their company, they will have information on how to contact the organization, group or company that worked on the matter, and could establish a liaison to find more information.

5.3.1.2 Homepage Maintenance

The Task Force further recommends that the NIIF create and maintain the site. It is recognized that the NIIF has its own site on the ATIS homepage and could fulfill this recommendation by establishing a single source as part of its existing site. The Task Group contemplated that the NIIF would establish the necessary liaisons with other organizations and industry groups both inside and outside of the ATIS ranks, to gather information on those industry efforts addressing interconnection and interoperability. The NIIF could then post this information on its website. The goal of this exercise is to establish a central repository for this kind of information. In some cases, this exercise may include a mere notice as to certain work ongoing in another organization. In other instances, it may include actual procedures developed by an industry group on how to address a specific issue. The Task Group, however, did not contemplate that the site would serve as a "chat" line for interconnection/interoperability issues. (Chat lines for this purpose are further discussed in 5.4.1). Rather, it is intended to serve as a place where important information would be gathered. It was also contemplated that ATIS and NIIF do what is necessary to publicize the existence of this site.

5.3.2 Key Learnings

Liaison For the Enhancement/Modification of the Network Interconnection Bilateral Agreement Template

Recognizing that the interconnection environment will evolve over time due to the introduction and influx of new service providers, heterogeneous networks and unique service deployments, it stands to reason that the Network Interconnection Bilateral Agreement Template itself be dynamic in nature and flexible enough to accommodate new elements as they become important.

In this regard, the Task Group considered where the responsibilities for maintaining, updating, publishing and distributing the template might reside. While information shared across industry segments, facilitated by a NIIF-supported process (as recommended above) to gather information which the Task Group recommends be published on the ATIS/NIIF website, could produce significant shared information, one of the first objectives of this exercise may be for the shared information to serve as a platform for maintaining the Network Interconnection Bilateral Agreement template itself. As an example, the liaison itself would bring issues affecting interconnection to the designated forum to ensure interoperability and avoid duplication. The Task Group contemplated that the process would become an ongoing one, whereby the template is continuously updated based on receipt of this information, and presumably improved as new issues surface and are shared through a liaison process. And as previously recognized, while an improved template may be one result, the liaison process could serve to facilitate other results such as defining additional standards needs, creating recommended practices, and generally sharing interconnection/interoperability issues and resolutions reached. Thus, it seems than an NIIF liaison process could also meet the objective of improving the template on a more regular basis and possibly serve other important purposes too. In looking at how to increase communications in this context, the use of a liaison process seemed a viable route to achieve the objective.

5.3.2.1 Ongoing Responsibility for the Network Interconnection Bilateral Agreement Template

As previously recommended above (in Section 5.2.2), the Task Force recommends that the NIIF be the overall template custodian. In addition, the NIIF should be directed to take a broader responsibility for the template, including the establishment of liaisons with other industry committees, forums, and organizations whose expertise would help maintain and expand the template as needed and as appropriate. Such candidates for NIIF liaisons are the Ordering and Billing Forum ("OBF") for those elements of the template which may have billing system impacts for service providers. Another example would be a liaison with Committee T1 on the national standards developed for interconnection or even a liaison with the National Cable Television Association to learn if any work in that organization would impact the templates and thus, warrant amending the templates. If there were no direct impact to the template, but information was provided by the cable industry on how they addressed an interconnection issue, it might be worth sharing via the homepage as discussed above. Where there are other groups which have responsibility for the matters within the template, the Task Force recommends that the NIIF seek out the appropriate liaisons with other industry groups as part of its responsibility for the template. As recommended, the NIIF should be the centralized keeper of the template.

5.3.2.2 Ongoing Dissemination of the Network Interconnection Bilateral Agreement Template

In addition to the immediate dissemination of the template as recommended in Section 5.2.2, it is important that the template be made available on a regular basis, particularly as changes are made. The Task Group recommends, at a minimum, that it be posted on the NIIF homepage. The Task Group suggests that other forms of dissemination should be considered by the NIIF. This activity will begin to centralize this important information.

5.4 INFORMATION SHARING

As is discussed in above, information which is generated and properly shared across the industry can be very useful in attacking interconnection issues, and the homepage billboard discussed in 5.3.1.1 will be a valuable resource. This section discusses some of the specific sources of information that have been identified by the Implementation Task Group.

5.4.1 Key Learnings

In this time of a highly dynamic telecommunications industry and fast paced change, there is a premium placed on the availability and sharing of information about interconnection issues. The Task Group recognized many venues in which to obtain this information, including policy and standards arenas, industry forums, trade associations, industry seminars, the multitude of websites, and bulletin boards. The Task Group also recognized formal and informal methods of sharing information on interconnection and interoperability. The purpose of this section is to provide some pointers as to the sources for and locations of some of this information. The Task Group further recognized that because of the quantity and variety of information, the multitude of sources, and dynamic nature of information, a complete examination (and listing) is not feasible.

The objective of this exercise is to provide pointers to start the information gathering process for those in search of interconnection and interoperability information.

There exists a myriad of telecommunications trade associations, industry forums and standards/specifications development organizations. Some sources of listings of these organizations are:

- Bellcore SR-3776 (Issue 3, March 1997) - Telecommunications Industry Catalog of Forums, Standards Bodies, and Associations.

- The NRC II document, *Key Telecommunications Related Standards Groups*, Section 12, Exhibit 2, of the NRC's "Report to the Nation" (http://www.fcc.gov/oet/nric), identifies a number of organizations involved in the standards setting process, and the reports of the Interconnection and Changing Technologies focus groups discuss relevant interconnection issues.

- The FCC website (http://www.fcc.gov/ccb/ccsites.html) has a wealth of information. The FCC's Common Carrier Bureau and/or the National Telecommunications and Information Administration (NTIA) also link to the following websites:

  - Information Resources on the Internet, maintained by the Jeffery MacKie-Mason at University of Michigan (http://www.spp.umich.edu/telecom/telecom-info.html).

  - Computer and Communications Entry Page, maintained by the Advanced Telecommunications Program, Lawrence Livermore National Library (http://www.ctr.columbia.edu.vii/2_index.html)

  - The Virtual Institute of Information, maintained by the Columbia Institute for Tele-information (http://www.ctr.columbia.edu.vii/2_index.html).

Other sources deal with more specific interconnection issues. For example:

- The California Public Utility Commission has a good description of the process of reaching interconnection agreements (http://callthemonit.com/details/puchead.html)

- The North American Numbering Council (NANC) was established by the FCC to assist in adopting a new model for the administration of the North American Numbering Plan (NANP). Its webpage, which is accessible from the FCC homepage, is a useful source of information on numbering. Other sources of information on numbering include the Industry Numbering committee (INC), and the North American Numbering Plan Administrator (NANPA), which is responsible for day-to day management of numbering resources.

- The Alliance for Telecommunications Industry Solutions (ATIS) (http://www.atis.org).

- An “LNP Primer” written by the Illinois LNP Committee (available in zipped format at http://www.ported.com).

Venues pointed to by the general sources include trade associations, forums, and standards/ specifications organizations.

Trade Associations represent their members (usually from a single industry segment) and provide services such as developing market statistics or publishing some form of periodical by which their membership is kept informed of industry activities. Examples of some of these telecommunications trade associations include:

ALTS - Association for Local Telecommunications Services (*)
COMPTEL - Competitive Telecommunications Association
CTIA - Cellular Telecommunications Industry Association (*)
NCTA - National Cable Television Association (*)
NTCA - National Telephone Cooperative Association
PCIA - Personal Communications Industry Association
SBCA - Satellite Broadcasting and Communications Association (*)
TIA - Telecommunications Industry Association (*)
USTA - United States Telephone Association (*)

(*) Starred entries have webpages that can be accessed from the Information Resources on the Internet website.

Industry forums provide an arena for discussion and resolution of numerous issues affecting the telecommunications network. One such forum is the NIIF, sponsored by ATIS. Other examples include the ATM Forum and the SONET Interoperability Forum (SIF).

Currently, standards and specifications in the US are developed by standards setting organizations, professional societies, trade associations, technical advisory groups, and others. The bulk of these standards are developed as part of a voluntary system based on the principles of openness and due process leading to consensus on the content of the standard. Much of the voluntary standards development system in North America is administered through ANSI, recognized by many of the US standards developers as the central coordinating body. ANSI and its member standards developers work under a defined set of procedures that provide criteria, requirements, and guidelines for coordinating and developing consensus on voluntary standards.

The Task Group discussed two other aspects of information sharing. The first aspect discussed what information needs to be exchanged with respect to existing interconnections. The second aspect discussed if it possible to improve the process of finding out whether anyone else has encountered and solved a given problem (and does not feel their answer is proprietary).

In implementing interconnection, service providers may encounter specific technical questions and want to know if others have found and solved these issues. Are there mechanisms for speeding the exchange of information among experienced personnel? The Task Group discussed

setting up some kind of bulletin board or "chat group" for exchanging information on implementing interconnection. There currently are some "chat groups" available in the industry. For example, the Virtual Institute of Information, maintained by Columbia Institute for Tele-Information, has an area to discuss interconnection on its site, but it is being used mostly to discuss policy information at this point.

Further investigation revealed significant issues with trying to set up a "chat group" specifically to answer technical questions about interconnection implementation. The information on the bulletin board is only as good as what the participants contribute to it. If no-one is in charge of or moderating the site, there is no check on the validity of the information posted. Users would not know how much to trust the information. Furthermore, if everyone is asking questions but no-one takes time to reply, not much "conversation" is really occurring. Publicity for the bulletin board is another issue. If no one knows about it, getting answers from it may be difficult. Thus the Task Group does not recommend the setting up of a "chat group."

5.4.2 Recommendations

5.4.2.1 Additional / Enhanced Starting Points

The Task Group discussed creating additional new "roadmaps" of information resources.

A few additions could be made to the sources of information to which the FCC's homepage provides links. For example, there does not seem to be a direct link from the Mackie-Mason site to the homepages of the various state PUCs, and some important trade associations are missing.

The Implementation Task Group encourages the FCC and these organizations work jointly to ensure that listings are posted on the FCC website(s).

5.4.2.2 Provider Resources area on FCC website

Currently the FCC maintains a Consumer Resources area on the Common Carrier Bureau website. This area has customer satisfaction reports, frequently asked questions, and access to other telecommunications sites. A similar area for telecommunications providers should be created. This area could use the same access to other telecommunications sites as the Consumer Resources Area does. It could have its own frequently asked questions. If appropriate, customer satisfaction reports on suppliers to telecommunications providers could also be made available.

5.4.2.3 Interconnection Primer

The Task Group suggests that trade associations develop primers on interconnection and interoperability issues as part of the educational programs that they provide for their membership. The NRIC report could serve as initial input into this process.

Attachment A - Cover letter and the list of recipients for the NRC II Templates

List of Recipients:

Alliance for Telecommunications Industry Solutions (ATIS)
Association of Local Telecommunications Services (ALTS)
Cellular Telephone Industry Association (CTIA)
Competitive Telecommunications Association (COMPTEL)
National Cable Television Association (NCTA)
Personal Communications Industry Association (PCIA)
United States Telephone Association (USTA)

Cover Letter:

Memorandum to: Personnel Involved in Technical/Operational Interconnection Agreement Negotiation

Re: Interconnection Agreements & NRC Templates

Early in 1996, the Network Reliability Council Task Group II (NRC II), a federal advisory committee of the Federal Communications Commission (FCC), issued two templates (attached) to serve as a tool for facilitating the technical aspects of interconnection agreements between network providers. These templates, namely the Network Interconnection Bilateral Agreement Template and the Network Interface Specification Template, were then distributed throughout the industry as part of a compendium of technical papers entitled "Network Reliability: The Path Forward". Because of the breadth and scope of the compendium, the templates may not have found their way to personnel involved in current interconnection agreement negotiations.

Now, the Network Reliability and Interoperability Council (NRIC), also an FCC federal advisory committee and the next generation of the NRC II, has assembled. This committee has been charged with providing recommendations to the FCC for members of the telecommunications industry to implement interconnection between various networks in a manner that promotes reliable, fully interoperable, and transparent services. One of the initial tasks of this new group was to review the NRC II templates in light of the experience gained by participants in local interconnection negotiations, as well as in the implementation of relevant provisions of the Telecommunications Act of 1996.

After some initial review by the NRIC's Implementation Task Group, it was felt that an immediate re-dissemination of the original templates is timely since many companies are now engrossed in the negotiation process. While the templates may not encompass all issues involved in negotiating every agreement, the information in these templates may be useful in highlighting issues that might be addressed in such agreements. In addition, re-dissemination of the NRC II templates can serve as a vehicle for soliciting input and suggestions on any further template work

in which the NRIC engages. Should you have any suggestions on modifying the existing template, please contact Andy Scott at 202-775-3637.

We hope that this information is helpful to you. You will be advised on any further template work that the NRIC accomplishes over the next several months. Any questions regarding these initial templates may be directed to the Network Installation and Maintenance Committee (NIM) of the Network Interconnection and Interoperability Forum (NIIF). The NIIF Director is Nancy Pierce, ATIS. Her contact information is: telephone 202-434-8824, facsimile number 202-393-5453, e-mail address npierce@atis.org. The NIIF, sponsored by the Alliance for Telecommunications Industry Solutions (ATIS), is a newly organized forum merging the work and the activities of the former Network Operations Forum (NOF), the Industry Carriers Compatibility Forum (ICCF), and the Information Industry Liaison Committee (IILC). The NIIF mission is to provide an open forum under the auspices of the Carrier Liaison Committee (CLC) to encourage the discussion and resolution, on a voluntary basis, of industry-wide issues associated with telecommunications network interconnection and interoperability which involve network architecture, management, testing, and operations and facilitates the exchange of information concerning these topics.

Further information on “Network Reliability: The Path Forward” is available on the world wide web at http//www.fcc.gov/oet/info/org/nrc/fg2. Further information on the NIIF is also available on the world wide web at http://www.atis.org.

Sincerely,
NRIC Focus Group 1 Implementation Task Group
Contact: Andy Scott, Chair (202-775-3637)

Attachment B - Network Interconnection Bilateral Agreement Template	**Check Off**
1.0 Requirements and Agreements for Provisioning Network Interconnection	
General Reference: NOF Reference Document Sections 1,2,4, and 9	
* - Tariff Identification	
- List of Services	
- Unbundled Elements	
- Explicit Forecasting Information	
- Direct Traffic	
- Subtending/Transition Traffic	
- Documentation Requirements	
- Service Level Agreements	
- Interface Specification	
- Service Provisioning Process	
- Specific Versions of Protocol and/or Interface Specifications	
- Network Interface Standards, Version Control (Backward Compatibility),	
Mandatory and Optional Categorizations	
* - Interface for Ordering/Pre-Ordering	
- Network Synchronization Planning/Design	
- Compatibility with Year 2000 Specifications	
- Specific References: GR 2945, ISO 8601	
- Ensure Compatible Date Formats on Interface	
- Compatibility of Expanded Use of Information Digits	
- Network Design Parameters	
- Network Administration/Operations Security Requirements	
- Specific References: T1 252, 233, 243, GR 0815, GR 1322	
- Access Methodology Requirements	
- Firewall Requirements	
* - OSS Interface Requirements	
* - Applicable Tariffs on Confidential Information	
- Data Connection Security Agreements	
- Authentication and Access Control	
* - Electronic Bonding Requirements	
- Message Sets Exchanged	
- Performance Parameters (Throughput, Availability, *etc.*)	
- Audit Requirements	

Network Interconnection Bilateral Agreement Template	**Check Off**
- Service Interworking Requirements	
- Re-Sale Related Services Requirements	
* - Operator Services/DA Routing and Branding	
- Unbundling Related Services Requirements	
* - Dialing Plan Requirements	
* - Network Element Requirements	
- Diversity Requirements	
- Route Identifications	
- Diversity Definition	
*- Special Routing Translations (SSP, STP)	
- Protocol Implementation Agreements	
- Specific References: TR 246, T1.114, T1.116, GR 317, GR 394	
- Timer Values	
- Route Set Congestion Messages	
- Optional Parameters	
- Switch Parameters	
- MDF Requirements	
2.0 Installation and Maintenance Guidelines, Procedures, and Responsibilities	
General Reference: NOF Reference Document Sections 1, 2,3, 4, 6, 7, 8, and 9	
- Guidelines for Meeting/Maintaining Performance Service Levels	
- Interface Specifications	
- MTBF/MTTR	
- Performance Thresholds (Tolerance Range)	
* - E911 Database Updates	
- Measures For Specific Service Classes	
- Monitoring and Reporting Mechanisms	
- Responsibility Assignments	
- Facility Assignment	
- Network Control	
- Documentation Requirements	
- Contact Numbers	
- Implementation Plans and Associated Milestones	

Network Interconnection Bilateral Agreement Template	**Check Off**
- Maintenance Procedures for Status and Trouble Reporting	
- Inter-Network Trouble Resolution and Escalation Procedures	
* - Contact Lists	
- Internetwork Contacts	
- Security Contacts	
- Emergency Communications Plan	
- Regional Emergency Preparedness and Response Program	
- Equipment Supplier Participation	
- Security Management Participation	
- Mutual Aid Agreements	
- National Security/Emergency Preparedness	
* - Tones and Announcement For Unsuccessful Call Attempts and Toll Warnings	
- Services Related Operational Guidelines	
* - Directory Listings	
- Number Portability	
- Interim	
- Long Term	
- National Services	
3.0 Interconnection Testing Procedures and Responsibilities	
General References: NOF Reference Document Sections 1, 2,3, 4, 6, 7, and 9	
and Internetwork Interoperability Test Plan Reference Document	
- Responsibility Assignments	
- Automatic Testing	
* - Pre-Cutover Inter-Network Connectivity Testing	
- Interoperability Test Results	
*- Process For Circuit Level Testing and Performance Analysis of Unbundled Network Elements	
- SS7 and Other Critical Interface Inter-network Compatibility Testing	
- Service Protocols/Message Sets	
- CCS Interconnection Questionnaires	
- SS7 Diversity Verification and Validation	
- Information Sharing For Analysis and Problem Identification	
- In-depth Root Cause Analysis of Significant Failures	
* - Failure Analysis Procedures	

- Root Cause Analysis Processes
- FCC Outage Reporting Criteria
- Service Configuration
- Protocol Tests
- Compatibility Testing
- Security Testing and Audits
4.0 Network Administration and Management Guidelines, Procedures, and Responsibilities General Reference: NOF Reference Document Section 6, 8, and 9
- Documentation Requirements
- Network Configuration
- Contact Numbers
- Network Administration/Operations Security Management
- Access Methodology
- Functional Partitioning
- Access Control
- Password Control
- Encryption Control
- Calling Party Number Privacy Management
- Security Bas Guideline For Interconnected SS7 Networks
- Network Traffic Management
* - Traffic Engineering Design Criteria and Capacity Management
- Alternate Routing Designs
- Call Blocking Criteria
- Network Rearrangement Management
- Logical
- Physical
- Diversity Requirement Management
- Specific Reference: Committee T1 Report No. 24 on Network Survivability Performance
- Synchronization Design and Company-wide Coordination Contacts
- Specific References: T1.101 Digital Facility Standard, BOC Notes on the LEC Network, and SR-TSY-002275
- Establish Conformance
- Identify Contacts

Network Interconnection Bilateral Agreement Template	**Check Off**
- Coordination Administration	
- Routing and Screening Administration	
- Network Call Routing Administration and Management	
- Firewall Administration and Management	
5.0 Network Transition Considerations	
General Reference: NOF Reference Document Sections 6 and 8	
- Growth/Consolidation of Network Elements	
- NPA Splits/Overlays/Rearrangements	
- Major Rehoming, Rearrangement Plans	
* - Transition to Use of Emerging or Future Technologies, such as SONET Interconnection,	
ODLC, and FTTC	
- Vendor Compatibility	
- Optional Capabilities	
- Feature Interactions	
6.0 Billing Considerations	
General References: Various documents available through the Ordering and	
Billing Forum (OBF)	
- Accuracy of Data	
- Interval of Records Exchanges	
- Dispute resolution	
*- Billing Records Data Exchange	
- EMR Standards	
- OBF Documentation	
7.0 Vendor Requirements and Responsibilities	
General References: Network Interface Specification Template as well as	
pertinent technical standards and documents developed by industry standards forums	
- Written Requirements	
- Software Validation	

Network Interconnection Bilateral Agreement Template	**Check Off**
- Optional Requirements	
- Testing	
- Training	
- Emergency Equipment Availability	
- Contact Lists	
- Interface Specifications For Standard Elements	
- Process For Certifying Combination, Intermingling, and Operation of NEs	

Note 1: NOF Reference Document referenced is Issue 12. Issue 13 is due for release 2Q97. Internetwork Interoperability Test Plan Reference Document referenced is dated 12/95.
Note 2: Items that are asterisked (*) may pertain to unbundling and/or resale. These may not be the only items pertaining to these issues.

Attachment C ATIS organization chart, directory, and contact information

ALLIANCE FOR TELECOMMUNICATIONS INDUSTRY SOLUTIONS, INC.
("ATIS")
1200 G Street, N.W.
Suite 500
Washington, D.C. 20005

ATIS Main Telephone Number (202) 628-6380
Main Fax Number (202) 393-5453

George L. Edwards, President & CEO	(202) 434-8820	gedwards@atis.
Susan M. Miller, Vice President & General Counsel	(202) 434-8828	smiller@atis.org
Megan Campbell, Staff Attorney	(202) 434-8847	mcampbel@atis.org
ATIS INFORMATION/PUBLICATIONS/MEMBER ADMINISTRATION		
Sally Freeman, Director-Public Relations	(202) 434-8850	sfreeman@atis.org
CARRIER LIAISON COMMITTEE (CLC)		
John Manning, Director	(202) 434-8842	jmanning@atis.org
COMMITTEE 05 (05)		
Harold Daugherty, Director	(202) 434-8830	haroldd@atis.org
COMMITTEE T1 (T1)		
Harold Daugherty, Director	(202) 434-8830	haroldd@atis.org
INDUSTRY NUMBERING COMMITTEE (INC)		
John Manning, Director	(202) 434-8842	jmanning@atis.org
INTERNETWORK INTEROPERABILITY TESTING COMMITTEE (IITC)		
Harold Daugherty, Director	(202) 434-8830	haroldd@atis.org
NETWORK INTERCONNECTION INTEROPERABILITY FORUM (NIIF)		
Nancy Pierce, Director	(202) 434-8824	npierce@atis.org
NETWORK RELIABILITY STEERING COMMITTEE (NRSC)		
William J. Klein, Director	(202) 434-8821	bklein@atis.org
ORDERING & BILLING FORUM (OBF)		
William J. Klein, Director	(202) 434-8821	bklein@atis.org
PROTECTION ENGINEERS GROUP (PEG)		
Harold Daugherty, Director	(202) 434-8830	haroldd@atis.org
SONET INTEROPERABILITY FORUM (SIF)		
Nancy Pierce, Director	(202) 434-8824	npierce@atis.org

TELECOMMUNICATIONS INDUSTRY FORUM (TCIF)

John Manning, Director	(202) 434-8842	jmanning@atis.org

TOLL FRAUD PREVENTION COMMITTEE (TFPC)

John Manning, Director	(202) 434-8842	jmanning@atis.org

6.0 OPERATIONS

MISSION

In response to Section 256 of the Telecommunications Act of 1996, the Operations Task Group (OTG) under Network Reliability and Interoperability Council (NRIC) Focus Group 1, has worked to identify the engineering and technical barriers to interconnectivity, interoperability, and accessibility to Incumbent Local Exchange Carrier (ILEC) Operations Support Systems (OSS) and Common Channel Signaling (CCS) resources and associated operational issues with performance monitoring, security, and interoperability testing. In addition, they have developed recommendations and processes for the industry and the Federal Communications Commission (FCC) to implement, to avoid or minimize those operational barriers.

PROCESS

Individually and as a team the OTG members reviewed the prior work and recommendations of Network Reliability Council (NRC) I and II that would be applicable to the effort. The teams also categorized the operational key issues identified by the Focus Group 1 Data Collection (Appendix E). Then subteam leaders were assigned to each of five key issue areas -- OSS Access, Signaling, Performance Monitoring, Security and Interoperability Testing -- to develop actions and study plans. The OTG together then reviewed several selected presentations by industry experts in each key issue area. This effort helped bring the team to a common level of understanding and helped identify several additional key contributors. Then the OTG broke up into subteams and created data items for each of the key issues. Although data items related to security of the Public Telephone Network of the Local Exchange Carriers, other data items specific to addressing the security issue were contained within the OSS Access and Signaling key issues discussions. These data items were posted on the NRIC web site for industry comment, using the template provided by the NRIC Focus Group 1. The OTG Core Team drove to consensus on all comments from industry and recommendations by a series of Task Group Reviews.

PROBLEM AND PRODUCT

The basic problem the OTG faced was promoting nondiscriminatory accessibility by the broadest number of users and vendors to critical telecommunications network resources (*i.e.*, CCS, OSS, network management systems, and mission critical network data) while at the same time maintaining the same high level of reliability and security that exists in the public telecommunications network today. The model for the recommendations that the OTG provided are in the operating zone of figure 1. The group deliberately avoided the bi-modal “extreme” recommendations of protect/certify and react/terminate service and chose instead a three step model of (1) set expectations/template and voluntary pretesting; (2) detect concerns/meaningful measurements and audit trails; and (3) notification and control/pre-agreed to triggers and actions

to safeguard the network. This paper and its recommendations are the combined product of the OTG Core Team and are offered to industry, government and the user community in the true spirit of cooperation and optimism that this difficult problem can be solved. In most cases, but most especially in the OSS access functional criteria, it describes the future end state at which the industry needs to be to fully support Section 256; not necessarily the immediate steps in the journey. The OTG believes successful access is being provided today and market forces will cause it to change over a period of time.

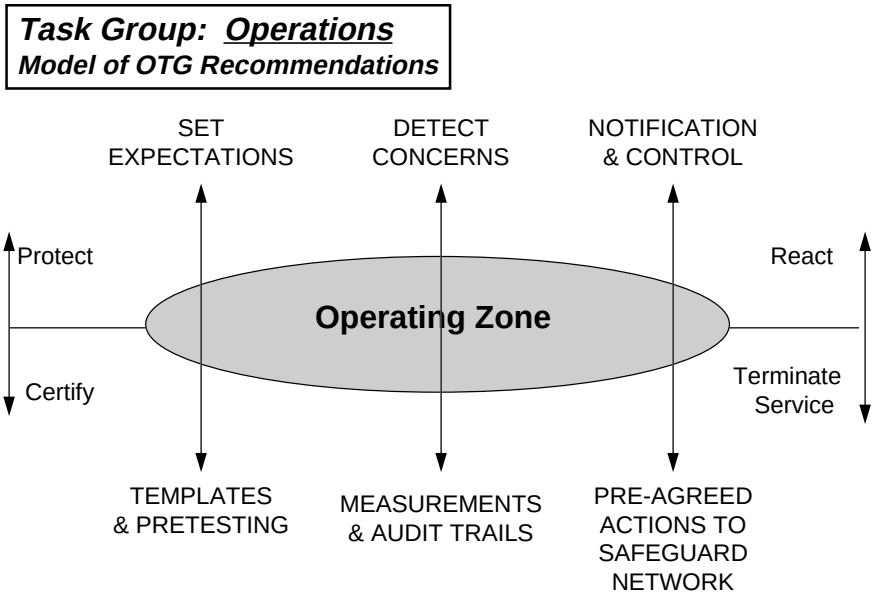


Figure 1

6.1 INVESTIGATION OF OSS ACCESS

The purpose of this section is to explore the issues associated with OSS Access.

The Federal Communications Commission (FCC) released CC Docket No. 96-98 on August 8, 1996 in compliance with the directive of the Telecommunications Act of 1996 to establish regulations to implement Section 251 - Interconnection Requirements. Additionally, the FCC amended the charter of the Network Reliability and Interoperability Council (NRIC) in order to "establish procedures for FCC oversight of coordinated network planning by common carriers and other providers of telecommunications services for the effective and efficient interconnection of public telecommunications networks used to provide telecommunications service, and may

participate in development by appropriate industry standards-setting organizations of public telecommunications network interconnectivity standards." Furthermore, it is the stated opinion of the FCC that "Section 251(c)(3) requires incumbent LECs to provide requesting telecommunications carriers nondiscriminatory access to network elements on an unbundled basis at any technically feasible point on rates, terms, and conditions that are just, reasonable, and nondiscriminatory. Incumbent LECs must provide requesting carriers nondiscriminatory access to operations support systems and information."

In response to the above directives, the Operations Task Group (OTG) under Network Reliability and Interoperability Council (NRIC) Focus Group 1, has worked to identify the engineering and technical barriers to interconnectivity, interoperability, and accessibility to Incumbent Local Exchange Carrier (ILEC) Operations Support Systems (OSS) and Common Channel Signaling (CCS) resources and associated operational issues with performance monitoring, security, and interoperability testing. In addition, they have developed recommendations and processes for implementation by the industry and the Federal Communications Commission (FCC) that will help avoid or minimize those operational barriers.

The various operations support systems currently being used by the ILECs were obviously not designed to be accessed by third parties without substantial changes. Each ILEC is, therefore, independently responding to the above mentioned order in a manner it believes will meet the directives of the order and that is sufficient to meet today's requirements. It is anticipated that the evolution of information technology, further identification of specific Competitive Local Exchange Carrier (CLEC) requirements, the growth of access requirements over time, and diversity of CLEC business plans will drive the need for additional gateway sophistication. These "drivers" and "enablers" will therefore guide the evolution of OSS access.

6.1.1 Gateway

The FCC Order in CC Docket No. 96-98, Paragraph 523, states "We thus conclude that an incumbent LEC must provide nondiscriminatory access to their operations support systems functions for pre-ordering, ordering, provisioning, maintenance and repair, and billing available to the LEC itself. Such nondiscriminatory access necessarily includes access to the functionality of any internal Gateway systems." As the needs for OSS access evolve, it is therefore anticipated that gateway functionality will evolve to meet these needs.

Although the gateway criteria identified below are described from an ILEC's perspective, it is recommended that the CLECs develop the mirror image of this gateway to effect efficient, secure transfers of information. Consequently, the evolution toward a sophisticated electronic gateway by the ILECs must be complemented by parallel development work by the CLECs to interface with these capabilities.

Key Learnings

When building this Gateway the following functional criteria must be considered:

- Functionality/Flexibility/Tuneability
- Computing Architecture Interoperability and Reliability
- Congestion Control
- Access Security

Recommendations

It is recommended that an electronic Gateway interface be developed and employed that meets the FCC Order in CC Docket No. 96-98, using the concepts of Telecommunications Management Network (TMN) Architecture and other applicable technologies.

6.1.1.1 Functionality/Flexibility/Tuneability

Given that an ILEC will be interfacing with multiple CLECs through an electronic Gateway, this Gateway will have to satisfy the FCC Order's functional requirements while being flexible, and tunable enough to meet the CLECs' needs.

The Gateway will need to deal with the following features while providing reasonable access methods for the CLECs:

1. Access To All OSS Functionality Types - The Gateway should provide the CLECs with access to Pre-Ordering, Ordering, Provisioning, Maintenance & Repair, and Billing.
2. Filtering Of Traffic Data Or Fields - The Gateway should be designed to allow the ILEC to filter out unnecessary or unauthorized data fields from a customer record.
3. Need For Local Service Request (LSR) and Electronic Data Interchange (EDI) Standards - The Gateway should meet all current and proposed LSR and EDI standards.
4. Isolation From Specific OSS Changes - When a change is made in an ILEC's OSS, the change should be transparent to the CLECs.
5. Interface To All OSS - The Gateway should interface, either directly or indirectly, with all of the necessary OSS functionality in a manner that will cause no more delay than absolutely necessary.
6. Allow for upgrades - The Gateway should allow for rapid implementation of upgrades that may occur due to new service offerings or new business arrangements that may evolve between the ILEC and CLECs.

Recommendations

- To facilitate meeting the FCC Order's functionality requirements, the Gateway will be subdivided into components and subsystems based upon business functions, interfaces, auditing functions and security.
- Though it may appear to be a single Gateway per access type to the individual CLEC, separate Gateways may be built to provide the required functionality to support the five business functions (pre-ordering, ordering, provisioning, maintenance & repair, and billing). This allows the architecture of the Gateway to have modular components. Based upon this

concept, flows between the individual components of the overall system can be identified and designed.

- The Gateway will be able to translate to a commonly agreed upon standard format (LSR standardized formats or EDI formats). These formats will be mutually agreed to and will be the basis of requests submitted to the Gateway to be communicated to the ILEC legacy OSS.
- The Gateway function represents a set of mediation services between an ILEC and the CLECs which provides for the exchange of data in agreed-to standard formats. EDI and the proposed LSR are potential candidates for this format. Because of its long history, EDI may be more prevalent for the pre-ordering, ordering, provisioning and billing business functions while a mix of EDI and managed object-based formats compliant with TMN and International Standardization Organization (ISO) standards will be used for the maintenance and repair functions.
- Whenever and wherever possible, data collected from one transaction through the Gateway should be available to populate a subsequent transaction through the Gateway, *i.e.*, data collected from a pre-ordering transaction will be used to populate an ordering transaction. The data should be buffered and populated by the CLEC originating the transactions.

6.1.1.2 Computing Architecture Interoperability and Reliability

The electronic Gateway interface should be developed using the most currently accepted computing architecture design standards in order to provide equal access for all CLECs. It should be recognized that once the Gateway is implemented and operational, any lack of availability of the Gateway will be service impacting to the users.

Since multiple CLECs will most likely use multiple computing environments that may or may not be similar to the ILEC's computing environment, the Gateway should be developed in a manner that will permit all CLECs to attach to the Gateway using an efficient method. This Gateway should also be developed in such a manner that it is maintainable in a technically secure environment.

<u>Key Learnings</u>

The following technical computing requirements have been identified:

1. Multiple Types Of Interfaces - The data communications interface between a CLEC and an ILEC should offer several protocols in standard languages in order to provide as many types of interfaces as reasonably possible and should be flexible to incorporate changes as standards evolve.
2. Routing Functionality - The Gateway should be designed in a manner that will permit and support multiple servers and transparent routing of transactions between servers.
3. Distributed Architecture - The Gateway should be built around a distributed computing architecture in order to take advantage of speed, reliability, recoverability, redundancy, *etc.*
4. TMN Compliant - The Gateway should be developed to meet all current standards with regard to TMN, Computing Architecture and other relevant standards.
5. Highly Programmable - The Gateway should be developed in a manner that will support changes, additions, or other modifications as easily as possible.

6. High Availability Platform - The computing platform should support current computing architecture standards in order to provide maximum reliability, recoverability, redundancy and throughput. The Gateway platform should not be vendor-specific so as to require a single source vendor.
7. Overload Protection - If an overload condition occurs, the Gateway should be fixable and recoverable in a manner that will be as transparent to the users as possible.

Recommendations

The electronic Gateway should be accessible through at least four network access subsystems. These are private line, dial-up, EDI, and Internet based access as appropriate for the various types of functionality. While it is recognized that OSI interfaces are at the core of telecommunications standards, it is recommended that use of the Transmission Control Protocol/Internet Protocol (TCP/IP) family be used for access to facilitate encompassing as wide a potential CLEC audience as possible.

- Private Line interfaces: Private line interfaces will be made available. This technology will be firewalled in such a way that the ILEC's and the CLEC's data are protected from one another. Where applicable, local address mapping may be applied to facilitate routing data to the electronic Gateway of the ILEC. Routing protocols used for this type of interface will be based upon Internet Engineering Task Force (IETF) standards with Open Shortest Path First (OSPF) or Border Gateway Protocol (BGP) preferred.
- Dial-up Access: Access to the Gateway will be made available by means of dial-up access. In-dials will be secured using the IETF proposed standard RADIUS methodology or secure ID Card technology. A variety of options relating to speed and technology will be afforded. ISDN access will be recommended because of its speed and versatility. Point to Point Protocol (PPPs) will be used over these linkages.
- Internet interfaces: Access to the Gateway will be available using the Internet. Access to the Gateway will be provided by means of a web interface. This technology will be firewalled in such a way that the ILEC's and the CLEC's data are secured from one another.
- EDI interfaces: Access to the Gateway is normally through a Value Added Network (VAN) using, as an example, X.25 protocol or dial-up. These interfaces are available through a variety of service providers.

Reliability:

The Gateway should provide continuous availability using High Availability technology with processor failover in the event of a processor failure or fully redundant subcomponent structure. Generally, failure of a module should trigger the initiation of a redundant processor to allow the system components to continue to operate. In addition, it is expected that these systems should reside in a 24-hour per day, 7-days a week (24x7) facility and should have battery backup and standby power systems. The computing architecture will support replacement of components without requiring the operator to power down the Gateway. System predictive monitors for failing components and multiple fault-tolerant processors are recommended in the Gateway design. Multithreaded operating systems are recommended where possible to ensure highest

performance in processing transactions. The computing architecture of the Gateway should be scaleable to allow for growth traffic and functionality.

6.1.1.3 Congestion Control

Recognizing that multiple CLECs will be accessing an ILEC's electronic Gateway interface continuously throughout the business day, a process must be developed that insures equal access for all CLECs.

Without some Congestion Control process in place, it is conceivable that a CLEC, either intentionally or unintentionally, could prevent other CLECs from accessing the Gateway. The ILEC should be responsible for ensuring that all CLECs have an equal opportunity to access the Gateway. The ILEC should also be responsible for monitoring the traffic across the Gateway in order to manage it and to maintain predetermined standards for flow-through.

Key Learnings

The following five areas of Congestion Control have been identified:

1. Trouble Detection - The situation in which traffic data reaches a level where service might be impacted and some action needs to be taken.
2. Prioritization - A scheme by which some predetermined traffic might take priority over other traffic regardless of the requesting CLEC. This includes prioritization by traffic type (inquiry versus activation), and by prior agreement of the CLECs.
3. Peak Traffic Requirements - How is the Gateway sized to handle busy-hour traffic or other load factors?
4. Traffic Engineering Parameters - What are the parameters for forecasting and sizing?
5. Service Related Impacts - When a mass outage occurs because of weather or other disaster, what changes in normal data traffic handling must occur?

Recommendations

- Ensure that each CLEC is afforded a choice of network access methods to the electronic Gateway.
- A software tool should exist to detect congestion problems within individual components of the Gateway(s).
- A software tool should exist to isolate problems affecting the Gateway and facilitate clearing the problem. This should be developed using TMN standards and other international standard technology.
- Provide a subsystem to document congestion in each access mechanization and report malicious activities to the FCC or appropriate authorities. Standards based network management tools, using Common Management Information Protocol (CMIP)/Common Management Information Services Element (CMISE) and Simple Network Management Protocol (SNMP), will be applied.
- A software tool should be provided to monitor telemetry and performance data in the Gateway and between distributed systems that the Gateway relies upon.

- Traffic and capacity of Gateway and access links will be modeled to identify probable bottlenecks and suggested data points.
- A traffic engineering module should be developed to determine blocking factors provided by current network access methods of the Gateway.
- A non-discriminatory access or queuing algorithm should be developed to accommodate unusual traffic patterns so that each CLEC has an equal probability of obtaining access into the Gateway during these events.
- Reporting software tools should be developed to document response time, congestion and Gateway usage for each CLEC.
- Software tools should be provided to document mean-times to resolution for alarms, for fulfillment of specific business function requests, and for comparisons of response times between an ILEC and a CLEC and between a CLEC and another CLEC.
- Insure that no single or group of CLECs is favored over any other CLEC or group of CLECs.

6.1.1.4 Access Security

As competing companies increasingly share systems and data, access to those resources must be secured. Without a full range of security measures in place, both systems and data are in danger of misuse, corruption, and loss of confidentiality.

Key Learnings

Among the ways information may be shared are EDI VAN connections, LAN-to-LAN connections, dial-in, and public Internet access. In every case, each party must ensure that:

- The entity on the other end is who it says it is;
- The entity on the requesting end is authorized to access the data and/or make changes; and
- The entity on the requesting end is prevented from accessing anything other than the authorized data.

Depending on the communications medium used for access, the degree to which the transaction must be secured will vary.

There will be various levels of security when partitioning data, including the following:

- Data records that are owned by one company that must not be viewed by another;
- Data records that are owned by one company that may be viewed but not changed by one or more other companies;
- Data *fields* that must be restricted in a record but residing in records that contain otherwise public information.

Regardless of the communications medium, these issues must be addressed.

Recommendations

Before any access security methods can be effected, agreement must be reached as to the kinds of data that will be shared. Customer confidentiality and proprietary data must be protected while common data must be readily available to all authorized users. It is recommended that the classification of the data be resolved by the CLECs and ILECs as quickly as possible.

There are many ways companies may share information including LAN-to-LAN connections, VAN connections, dial-in connections, and public Internet access. The degree to which each of these must be secured varies. Key facets to secured transactions are identification, authentication, access control, data integrity, data confidentiality and non-repudiation. It is recommended that Access Security reach the High Level of Security Requirements contained within ANSI T1, 233, 243, and ITU-T.

Encryption will be central to several aspects of security. It can serve as safeguard against unauthorized recipients interpreting transmissions, thereby protecting confidentiality and preventing fraud. It can limit damage caused by an individual or system entering a command, intentionally or otherwise, that destroys a file system. Encryption can provide authentication of the message originator and the system user. Electronic certification and digital signatures can protect against unauthorized modification and forgery of documents.

No encryption is recommended for LAN-to-LAN or VAN communications so long as the LAN, VAN or environments in between are reasonably secured to industry standards such as the ANSI T1 233, Bellcore *Generic Requirements For Data Communication Networks,* TR-STS-0001332, *etc.*. For dial-up or Internet access, a more sophisticated process algorithm will be a necessity. Secure Socket Layer (SSL), Secure Multipurpose Internet Mail Extensions (S/MIME), secure IP tunneling, and X.509 are examples of accepted methods for providing confidential exchanges on the Internet; an equivalent solution is recommended for dial-up. While these methods may affect the throughput of transactions, anything less is subject to interception and interpretation by unauthorized parties. It is further recommended that vendor-proprietary algorithms should be avoided because they frequently have not been subjected to a thorough industry-wide analysis.

Authentication involves establishing a proof of identity. The most common element of authentication involves the use of user identification and password. With any connection, some form of ID/password is crucial. With dial-in and public Internet access, the use of one time passwords, a security calculator or "smart card" is recommended. Further, encryption of the user identification and password is critical when data is transmitted over the public network via dial-in or public network access.

The trusted third party concept is essential to authentication. With a trusted third party, neither the user nor the host relies solely on the credentials supplied by the other. Instead, each relies on a third entity called a Key Distribution Center (KDC), to vouch for the other. The KDC alone bears the burden of trust because all parties trust it and not each other. While most implementations of KDC involve asymmetric encryption, there is no reason why it may not be used for symmetric encryption as well.

Hand-in-hand with authentication is the identification of the privileges accorded each user for access control. These privileges will govern what transactions a user may submit and what data that user is permitted to see.

Access control and data partitioning relates to whom or what may have access to data and resources to protect competitive information, data, and systems. Since identity is at the core of

access control, its implementation requires some form of authentication. For example, there will be data that can be viewed by all parties but changed by only one. Similarly, there will be data that can only be viewed by a single organization. In that vein, data that may be viewed by a single company may be limited to a subset of individuals within that company. While the access control policies should be constant across all access methods, implementation may vary.

Filtering must be done on both incoming requests and their responses. For example, access by an unauthorized party should be recognized at the Gateway when it arrives and should be rejected immediately. Other filtering will be required for each message response. For instance, accesses by an otherwise authorized entity to another organization's company-specific data will be monitored and checked before it leaves the Gateway; an unauthorized access message will be returned instead of the requested data. Proxy firewalls combined with packet filtering routers provide a strong combination; other products such as configuration management products, virtual private networks, network address translation processes will provide additional functionality and security.

For data field security and record level security, it is recommended that a test be made to ensure that the company is authorized to receive the requested data. For transaction level security, a mapping must be made to the specific user within a company and may be implemented either when the message arrives or before the response is returned by the Gateway.

Non-repudiation and intrusion alert logging must be provided regardless of the point at which access control is exercised. It is recommended that the logging be done in a consistent fashion at both the Gateway and the data source.

Integrity applies to guaranteeing that what arrives is identical to that which was sent and that only the intended recipients can access the contents. Encryption and access control combined with reliable transmission facilities will ensure that this goal is met.

6.1.2 Audit Trails

In order to track information exchanges between CLECs and ILECs, audit trails of all transactions through the Gateway must be established.

Audit Trails are necessary to ensure the integrity of the information exchanged between the originating and responding parties. The audit trail must provide multiple functionality to support other functions related to OSS Access such as security, backup and recovery, Customer Interface Agreement compliance, and nondiscriminatory access proof.

Recommendations

It is recommended that an automated Audit Trail be established within the Gateway for all OSS access information exchanged between the CLEC and ILEC to provide proof that all Customer Interface Agreements have been met. The Audit Trail should provide the following functions:

- Transaction accounting at the Gateway - In order to track which CLEC sent a transaction across the Gateway, what was the transaction, who in the CLEC made the transactions, when it was made and how far the transaction went into the ILEC OSS, all transactions must be logged.
- The audit trail of transactions will be made available for viewing by each CLEC for its transactions and only its transactions.
- Changes to administrative data - If changes occur to a field on a customer record or if permission to change that field occurs, the audit trail must identify who made the change and when it was made.
- Detection of unscrupulous business practices and misuse - A scheme should be developed to identify if a CLEC or an ILEC attempts to block out other parties by overloading the Gateway with in-bound or out-bound traffic.
- Intrusion detection and attempts - If a CLEC or ILEC attempts to view or change a customer record without permission, the attempt must be logged in the audit trail.
- Proof that access is nondiscriminatory - The audit trail should be available to authorized parties in order to prove that traffic data are nondiscriminatory.
- Insurance of Customer Interface Agreements - The audit trail should be designed to provide proof that Customer Interface Agreements reached under Section 6.1.5 are met.

6.1.3 Information Exchange Associated with OSS Access

Because multiple CLECs will need to exchange information electronically with multiple ILECs, it will be necessary for the CLECs and ILECs to reach a common understanding of the definition of functions and data items.

Since it is expected that the CLECs and ILECs will be using their own internal Operations Support Systems, then it is expected that functions and data items will not be initially defined in the same manner. If an ILEC requests a particular function be performed or asks that it be sent a particular data item, the receiving CLEC must have a complete understanding of what is requested, and the ILEC must have a complete understanding of what is returned.

Recommendations

A “common language” should be utilized to facilitate interactions and flow thru by using previously agreed upon and published ANSI standards, and definitions of business area functions and data types and attributes.

6.1.3.1 Common Understanding of Functions

In order to comply with the FCC Order to provide nondiscriminatory access to OSS functionality, the CLECs and ILECs must reach a common understanding of specifically what functions are performed by the OSS and how they relate to their business processes.

The five major business areas defined in the FCC Order, (Pre-ordering, Ordering, Provisioning, Maintenance & Repair and Billing) will most likely not be performed in exactly the same manner or contain exactly the same data between any of the CLECs or ILECs. Therefore, it is imperative that a common understanding be reached of what business processes are being performed by the ILECs OSS and what data will be returned before a CLEC accesses the ILEC's OSS.

Recommendations

It is recommended that whenever possible a previously agreed upon and published definition for a business area function be used to describe that function. As an example, the Bellcore document "BOC Notes on the LEC Networks" glossary contains a significant number of the definitions used in this document. Bellcore publication SR-TSV-002275, Issue 2, April 1994, which is currently being revised, is available to the public for purchase. In addition the Bellcore COMMON LANGUAGE[36] Standards such as BR 751-100-460, COMMON LANGUAGE SWITCHING SYSTEM CODES, provide the industry with a common set of definitions applicable to circuit administration, provisioning, design, and engineering considerations for switching system network elements. This and other Language Standards BRs are described in Bellcore publication SR-4302, entitled LANGUAGE STANDARDS SUMMARY OF PUBLISHED PRACTICES. Also, the Ordering and Billing Forum (OBF) at the direction of Alliance for Telecommunications Industry Solutions (ATIS) developed the "Local Service Ordering Overview", SR-STS-471070, document which contains a description of data and functions related to Ordering and Billing. Both of these documents are publicly available through Bellcore.

6.1.3.2 Common Understanding of Data Types, Definitions, and Attributes

In order to comply with the FCC Order to provide nondiscriminatory access to OSS functionality, the CLECs and ILECs must reach common agreements on data types, definitions, and attributes.

The five major business areas defined in the FCC Order, (Pre-ordering, Ordering, Provisioning, Maintenance & Repair and Billing) will most likely contain similar terms in discussing data, but it is unlikely that these terms will mean exactly the same thing to every CLEC or ILEC. Therefore, before a CLEC accesses an ILEC's OSS functionality, the CLEC must understand the data terms (types, definitions, and attributes) of what they are requesting and what they will receive from the ILEC.

[36] COMMON LANGUAGE is a Registered Trademark of Bellcore

Key Learnings

- Wherever possible, established standards from other references, such as American National Standards Institute (ANSI), OBF, Electronic Communications Implementation Committee (ECIC), T1M1, should be used to define these terms.
- If there is not an established standard definition for a particular data term, it should be developed by ATIS.
- A working agreement should be developed to pursue these definitions in an ongoing environment.

Recommendations

It is recommended that whenever possible a previously agreed upon and published definition for a business area data type be used to describe that data type. As an example, the Bellcore document "Carrier Access Billing System (CABS), Billing Output Specifications, Volume 4, Data Elements" contains a description of most, if not all, of the data types needed to address these Issues.

This document, SR-OPT-001874, is a public document that may be obtained from Bellcore.

6.1.3.3 Applicable ANSI Standards

The following is a list of American National Standards developed by Committee T1 that could be used in developing a common understanding of the Gateway:

ANSI T1.214-1990 Generic Network Model for Interfaces between Operation Systems and Network Elements

ANSI T1.224-1992 Protocols for Interfaces between Operation Systems in Different Jurisdictions

ANSI T1.246-1995 Information Model for Services for Interfaces Between Operations Systems Across Jurisdictional Boundaries to Support Configuration Management - Customer Account Record Exchange

ANSI T1.228-1995 Services to Interface Between Operations Systems Across Jurisdictional Boundaries to Support Network Management (Trouble Administration)

ANSI T1.227-1995 Extensions to Generic Model for Interfaces Between Operation Systems Across Jurisdictional Boundaries to Support Fault Management and for Standardized Protocol Interface (Called the "Q3" Interface in the TMN)

ANSI T1.201-1993 Lower Layer Protocols for TMN Interfaces Between Operation Systems and Network Elements

ANSI T1.208-1993 Upper Layer Protocol for TMN Interfaces

6.1.4 Performance Measurements

The performance of the Gateway will be crucial to the flow of transactions between an ILEC and CLECs. There are two main measures of performance:

1. Throughput or the rate at which the Gateway can process requests and
2. Response Time or the time it takes to process one request.

The following factors affecting performance will depend on a number of subsystems present in the Gateway subcomponents:

- Network Access Speed and Throughput,
- Network Input/Output (I/O) into the Gateway subcomponents,
- Memory of the Gateway subcomponents,
- Disk I/O of Gateway subcomponent, and
- Central Processing Unit (CPU) subsystems employed in the design of the Gateway.

Because the performance of the Gateway system as a whole depends upon the aggregate performance of the subcomponents used to build the architecture; overall performance of Gateway systems must center upon providing comparable throughput and response time across each access method. These comparisons should be made between ILEC and CLEC for transactions which are representative of the five core business functions between like modalities of architecture. A small CLEC choosing to implement network subcomponent access to the Gateway using a 9.6 modem dial-up should not expect the same performance of a CLEC who chooses to implement a DS-3 private line connection to the Gateway. Comparisons should be made to like modalities of access, security, and transaction architecture.

Recommendations

- A set of standard performance criteria should be developed by T1A1 that will initially seek to offer performance specifications for subcomponents of the Gateway and will guarantee minimum performance levels for each transaction type using specific subcomponents. These criteria should be established by testing and benchmarking.
- Unique performance requirements may be negotiated between CLECs and ILECs and documented in the bilateral agreements.
- A set of performance telemetry data for subcomponent types will be mutually agreed to and made known to all interested parties at a mutually agreed to frequency and granularity.

6.2 SIGNALING

There is a rich history associated with the interconnection of telecommunications networks at common channel signaling network interconnection points utilizing SS7 protocols and

procedures. There are many examples of interconnected network carriers in operation today that provide users transparent, effective, seamless services. Local Exchange Carriers, Interexchange Carriers and now wireless carriers are providing integrated services to their subscribers utilizing common channel signaling infrastructure. In some cases third party signaling service carriers provide signaling connections between two signaling end points operated by two different exchange carriers. NRC II, in its report "Network Reliability: The Path Forward" (April 1996), provides background and analysis on issues and concerns related to interconnecting networks and provides recommendations on how to enhance efforts to improve the building of reliable interconnected networks.

Sophisticated test plans have been developed and implemented within the industry that have provided a comprehensive framework for the interconnection of common channel signaling networks and the interconnectivity of associated devices. Much of this work has been accomplished within the ATIS/Network Operations Forum (NOF) and will now be expanded upon within the newly formed Network Interoperability and Interconnection Forum (NIIF) that supersedes NOF and has an expanded mission. Many of the issues addressed and resolved by the NOF are contained within the NOF Reference Document and other NOF issued documents. The NOF developed the Internetwork Interoperability Test Plan (IITP) and the IITP Reference Document as a vehicle to enhance network reliability in a multi-vendor, multi-carrier environment. By participating in IITP activities and performing the associated network level interoperability testing vendors and carriers have achieved a demonstrated high level of signaling network reliability. In most cases the NOF reacted to identified weaknesses within the common channel signaling network. The NIIF should be more proactive. It should look at new SS7 applications and issues such as security that will impact quality of service as an increased number of service providers are interconnected via the signaling infrastructure.

Within service contracts between public carriers, bi-lateral agreements are reached through the utilization of interconnection templates, the citing of established and proven standards and test plans, and agreements that explicitly define the detailed processes and procedures that ensure long term reliable signaling network planning, implementation and operation. NRC II developed tables of generic criteria that assist in identifying a minimum list of characteristics that must be addressed to establish and maintain a point of interconnection between two networks. These tables, or templates, are made available as starting points in the generation of the bi-lateral agreements entered into between interconnecting service providers.

Though signaling network interconnection and interoperability procedures and processes can be classified as well-defined and stable in their current network application, there are potential barriers that may hinder the full realization of an accessible, reliable, open, trusted environment, to the broadest number of users and vendors of communications products and services.

The categories of potential barriers, identified by industry, to signaling network accessibility, interconnection and interoperability that may affect the continued robustness of the signaling network are:

1. **Experience Level** - Inexperienced service providers may not fully realize the complexity of network operational practices that are required to ensure network integrity (*e.g.,* synchronization and link congestion issues).
2. **Open Networks** - Mandated opening of network resources will require new network capabilities and functionalities affecting signaling network services (*e.g.,* Local Number Portability (LNP), Intelligent Network (IN)/ Advanced Intelligent Network (AIN) unbundling). With this are issues related to the ownership of resources, co-location rights and inter-carrier compensation for services rendered.
3. **Network Evolution** - Market and technology driven evolution of the signaling network in a multi-service provider environment needs to be managed to accommodate technology advancement, standards development, new national/global service offerings, carrier differentiation, and vendor differentiation.
4. **Quality of Service (QOS)/Performance** - Quality of inter-carrier service offerings with signaling network performance verification along with accountability rules and dispute resolution. Issues may involve real-time, near real-time and long-term actions by service providers.
5. **Security** - Security of the signaling network in a multi-carrier interconnected environment that ensures the integrity of all access points to the signaling network including signaling links, embedded operations channels, OSS access interfaces and Gateway screening firewall capabilities that go beyond the existing address checks into message content and buffering of harmful message content.[37]
6. **Network Reliability** - The need for expanded internetwork Gateway services and the criteria for when signaling messages must be/can be/cannot be discarded and what information elements or reports should be generated and shared across network boundaries. Administration and maintenance activities affecting interconnected networks can present substantial network reliability risks.

To overcome the barriers presumed within the identified potential barriers and to ensure the continued reliability, performance and security that is the hallmark of today's

[37] One or more significant security holes have been identified which could potentially lead to wide spread service degradation and reportable outages among multiple interconnected carriers:

- Exploitation of new or existing security holes in deployed or developing CCSSO, SSP, SP, STP or DCS systems or their environmental support systems to affect software manipulations *e.g.,* worms, time bombs, database corruption affecting translations or program code performance
- Protocol manipulation to affect congestion through SS7 message interception and modification
- Manipulation of SEAS or other translation affecting Operations Systems *e.g.,* affecting mated pair translation anomalies or uneven/non-existent link set priorities on routing or routing sets
- Physical compromise of the STP, SSP, SP or CCSSO backup media coupled with one or more of the above scenarios
- Network Management message spoofing or replay *e.g.,* TFAs, TRFs, TFPs, TFCs
- Point code manipulation and spoofing.

telecommunications networks, there may be a need for architectural adjustments to the SS7 network, *i.e.,* message looping in LNP.

6.2.1 Experience Level

Inexperienced service providers may not fully realize the complexity of network operational practices that are required to ensure network integrity.

Key Learnings

Issues:
Service providers new to signaling operations procedures may unknowingly engineer or operate signaling elements and links in ways that could negatively impact network reliability.

Background:
Some operational practice areas that influence signaling network integrity are as follows:

- Link set capacity and engineering rules
- Awareness of checklists and rules
- Understanding and interpretation of cause codes
- Synchronization and timing

Recommendations
It is recommended that new service providers be encouraged to participate in NIIF and Network Testing Committee (NTC)/IITP or equivalent Interoperability activities and when applicable perform the associated network level interoperability testing defined within the test plan.

It is recommended that, to avoid potential problems related to synchronization and timing, new carriers follow the recommendations stated in section 5.1.2.5, section 5.2.2.5 and section 5.4.2.5 of the NRC II report "Network Reliability: The Path Forward," April 1996.

It is recommended that ATIS/NIIF or equivalent consensus based forum manage a database of relevant industry information that would assist new entrants in becoming aware of the availability of such information and how to obtain this information. The database could contain abstracts and pointers to information such as the NIIF interconnection template contained in the NIIF Network Operations Document (NOD) (formerly NOF Reference Document) and the new SS7 Cause Code Reference Manual contained in the NIIF NOD. (See Section 5.3.1.)

6.2.2 Open Networks

Mandated opening of network resources will require new network capabilities and functionalities affecting signaling network services (*e.g.,* LNP, IN/AIN unbundling). With this are issues related to the ownership of resources, co-location rights, and inter-carrier compensation for services rendered.

6.2.2.1 National Requirements

Key Learnings

Issue:

There is a clear need for coordinated network service and network interface requirements but it is not clear who owns/generates national telecommunication requirements that can gain support from a broad range of service providers.

Background:

ANSI provides standards, not requirements (note: standards define a framework but do not have to be implemented and may allow many variations on an implementations). Bellcore has published SS7 requirements and is probably the only source of public requirements for Signaling Transfer Point (STP) Gateway Screening. However, there are apparently no public requirements published and claimed to represent all points of view (LEC and IEC).

The NIIF will address issues related to definitions of interoperability that address matters associated with the implementation of standards. The NOF addressed many of these issues related to SS7 protocol. The NIIF is chartered with this ongoing work.

Recommendations

It is recommended that the NIIF lead this work. It is further recommended that the NIIF should continue to place a high degree of focus on SS7 inter-network interconnection and interoperability by assuring adherence to, and providing clarification of, applicable standards. Industry participants should provide early detection and reporting of signaling network operational issues and performance information to the applicable NIIF group to help contribute to timely resolution and corrective action, thus improving network reliability.

It is also recommended that the planning process, as illustrated within the Planning Section of this document, be followed to ensure reliable signaling network interconnection and interoperability. (See Section 4.)

6.2.2.2 Network Testing

Key Learnings

Issue:

There is a need for coordinated LNP signaling network testing.

Background:

There are resident safeguards to protect the SS7 network that have been derived through industry forums and/or standards committees. With the implementation of LNP, new scenarios of call configurations will be introduced into the existing network. In order to ensure continued network integrity, applicable test scripts are in the process of being identified in multiple working groups.

The IITP, which has now become the Network Testing Committee of the NIIF, is the primary source of the establishment of the test scripts in question. The Illinois Commerce Commission and reportedly other state-sponsored groups are individually performing similar LNP testing activities.

Recommendations

It is recommended that the NTC of the NIIF should initiate liaison with all identified parties (both public and private) chartered to develop LNP testing processes and procedures. These parties should be encouraged to participate in NTC activities to ensure synergies to enhance the identification and correction of signaling and other SS7 problems such as security and integrity of network management messages before they are introduced into the network. The NTC should encourage reports, white papers and/or common meetings so that individual test configurations, processes, procedures, and results could be shared.

6.2.3 Network Evolution

Key Learnings

The evolution of the signaling network in a multi-service provider environment needs to accommodate technology advancement, standards development, new national/global service offerings, carrier differentiation, and vender differentiation. New market driven service providers will require new inter-network signaling capabilities due to the nature of their local, regional, national, or global service offering or service offerings (*e.g.,* wireline vs. wireless services). Their market expectation will be to provide service differentiation to their subscribers.

Issue:

With increasing numbers of service providers, significant signaling network technological/architectural changes will be required in support of increased service capacity and evolving functionality. The required changes may not occur as fast as service providers and their

customers would like. There needs to be a process for new market driven services and protocols to be introduced into the historically standards/reliability driven environment.

Background:
New markets emerge that can exert forces that change the way services are provided to subscribers. These new services often emerge on stand-alone networks that support the needs of the offered service. At some point it becomes necessary to interwork and/or integrate these new capabilities with established services and networks. A good example is the cellular network and its effects on the common channel signaling network. As wireless services grew, new standards affecting signaling have been developed causing changes to traffic types and flows. To accommodate these types of changes the signaling network cannot become so rigid in its operation (e. g., Gateway screening that is inflexible) that it becomes a barrier to new services.

New service providers will require new inter-network signaling capabilities that enable their new local, regional, national, or global service offering or service offerings. Their market expectation will be to provide service differentiation to their subscribers. Signaling network services requiring buy-in and deployment by increasing numbers of service providers are more difficult to bring to the market than services unique to one service provider.

The signaling network and its operation have historically been driven by standards. With opened interfaces, new services may be possible, but difficult to initiate in a relatively rigid environment. An example is how to provide/report billing information for a signaling network based database service.

<u>Recommendations</u>
Rely on normal competitive environment and market forces for providing new features. New carriers, sponsoring new signaling network capability initiatives, should utilize the Service Planning Process, as defined within the Planning Section of this document, well in advance of deployment target dates so that the appropriate development process can be achieved. (See Section 4.)

The FCC may need to initiate timetables for compliance to provide features for new national or mandated services when it becomes clear that sufficient progress is not being achieved to reach the goals set by Section 256 of the Telecommunications Act of 1996. In addition, for current LNP implementation, each local service provider owns an entire NXX for its switch. Concern has been expressed that this will lead to NXX exhaust and subsequent NPA relief. Therefore, there should be some coordination between the LNP implementation and the overall numbering plan. The FCC has established a federal advisory committee that is addressing numbering issues, the North American Numbering Council. We recommend they consider this issue.

6.2.4 Quality of Service and Performance

These issues pertain to the quality of inter-carrier service offerings in terms of signaling network performance verification, accountability rules, and dispute resolution. The issues may involve real time, near real time, and long term actions by service providers.

6.2.4.1 Interconnectivity Performance

Key Learnings

Issue:

Increased carrier interconnectivity and new mandated network requirements such as LNP are likely to lead to significantly increased signaling network (signaling elements and signaling links) capacity and performance needs.

Background:

Signaling network elements such as the Signaling Switch Points (SSPs), STPs, and Service Control Points (SCPs) (IN Databases), and the signaling links interconnecting them, will likely be required to transport and process an increased number of transactions per second as internetwork services and LNP are deployed. With significant increases in message transport capacity, the need for high speed signaling links will become apparent. In terms of the signaling network elements, both signaling link termination capacity and signaling message transaction performance requirements will be affected. To be effective in ensuring that the signaling network QOS does not degrade and provides consistent services as defined within carrier bilateral agreements for all interconnected parties, appropriate service measurements must be available to the interconnected parties.

Recommendations

It is recommended that signaling network test plans defined by the NTC be enhanced to include interconnectivity testing to verify minimum performance levels of signaling services provided by associated network elements including SSPs, STPs, and SCPs.

It is also recommended that standards bodies and service providers evaluate signaling network element (SSP, STP, and SCP) functionality in terms of transaction and link capacity and performance, operations, administration, maintenance, provisioning, database consistency and inter-network coordination, to determine the most efficient means of distributing or combining this functionality in network elements where appropriate per application. Signaling network architectural alternatives or enhancements to existing functional capabilities may be considered to relieve performance issues through more efficient utilization of network resources.

It is also recommended that T1A1 evaluate current performance measurements and make recommendations for additional measurements appropriate for the new multicarrier environment.

It is recommended that equipment providers be alert to the needs of the network and, in coordination with service providers, plan for network upgrade in a timely manner. Significant

improvements in technology and the application of technology through the utilization of the proposed planning process should help alleviate this problem as the network evolves.

6.2.4.2 Multiple Service Provider Problem Resolution

Key Learnings

Issue:

As interconnectivity increases greatly with additional new service providers, problem resolution from the end-customer's viewpoint is an issue.

Background:

Customer satisfaction can be greatly influenced by the QOS experienced in normal use of the network. The QOS can be affected by events or faults in down line carrier's networks that are interconnected to provide end to end services. An example could be a faulty signaling network segment that is not visible to the initiation service provider.

Network Interconnect (NI) Operations, Maintenance, Administration Part (OMAP), currently specified by ANSI T1 in Protocol Specification T1.116, defines procedures to find and diagnose inter-network problems -- *e.g.,* having MTP Route Verification Test (MRVT)/SCCP Route Verification Test (SRVT) in all network elements (intra-network and inter-network) would support route provisioning verification to agreed on network interconnections. It is recognized, however, that Network Interconnect Operations, Maintenance, Administration Part (NI OMAP) is not currently supported by all network service providers for various reasons.

Recommendations

It is recommended that the appropriate standards bodies review the existing standards and request contributions to help define specifications for interconnectivity testing and tools where existing procedures are insufficient.

It is also recommended that the FCC review the progress of this activity and set timetables, if appropriate, for implementation of a set of internetwork fault diagnostic procedures.

6.2.5 Security

Security of the signaling network in a multi-carrier environment ensures the integrity of all access points to the signaling network including signaling links, embedded operations channels, and other OSS access interfaces and Gateway screening firewall capabilities that go beyond the existing address checks into message content and buffering of harmful message content.

In addition, the potential exposure brought about by procedural errors affecting security during CLEC implementation of various mandates within the Act, *i.e.,* Local Number Portability, combined with the likelihood of the exploitation of these "windows of vulnerability" suggest that

affected carriers and vendors should reinforce their defensive, detective and reactive security capabilities and resources to deal with the increased risk.

6.2.5.1 Expand NIIF Document for Security

Key Learnings

Issue:

Security risks are significantly increased as many more signaling networks are interconnected at all levels of link types. Communications channels and interconnection to non-SS7 networks including the Internet via protocol converters for signaling network management provide additional security risks. Therefore, there is a need to enhance signaling network security and firewall robustness at Gateway screening functionality.

Background:

Potential barriers associated with signaling network security issues are currently addressed in-part by existing bi-lateral agreements, application of industry best practices, standards and NRC templates that reference the NIIF Network Operations Document, Section 9, the Security Base Guideline for interconnected SS7 networks. With respect to the gaps in security, there is a need to provide partitioned secure access to signaling OAM&P systems and networks. Likewise there is a need to strengthen firewall robustness at Gateway screening functionality. Many of the recommendations contained within the NRC II, Increased Interconnection Task Group II Report, dated January 14, 1996, reflect and support the path forward to address security.

Recommendations

It is recommended that the NIIF expand the Bilateral Interconnection Template (NIIF Issue 0014) to reflect the Security applicable best practices, standards (Committee T1), base guidelines (*e.g.*, NIIF Network Operations Document Section 9) and Data Connection Trust Agreements.

It is also recommended that the appropriate standards groups, service providers and equipment suppliers be strongly encouraged to apply the recommendations from NRC II as they relate to security issues with particular emphasis on firewalls.

6.2.5.2 Unauthorized Access (Hacking) Protection

Key Learnings

Issue:

Internetwork security may be at risk due to unauthorized access or information requests from within a connected network that are beyond limits of established bi-lateral agreements or the Gateway Specifications of ANSI Committee T1.

Background:

Unauthorized activity may appear as attempts through connecting networks to "learn" or "discover" network capabilities/topology, *etc.*, by "bogus" messages having no authorized

purposes as contracted between the interconnecting networks (*e.g.,* query a database to build an identical image of a target database). It may not be possible to detect and prevent this type of activity within the signaling network directly. Applications within signaling points (*e.g.,* SCPs) may have to provide the detection and protection that is needed.

Recommendations

It is recommended that T1S1 and/or T1M1 be requested to investigate this issue and provide additional Gateway firewall specifications and recommendations that would detect and report the existence of potential unauthorized signaling activity.

6.2.6 Reliability

Signaling network reliability becomes an issue as new carriers gain access to signaling network services. The multiple carrier environment creates a need for expanded internetwork Gateway services and criteria for when signaling messages *must be/can be/cannot be* discarded, and what cause information elements or reports should be generated and shared across network boundaries.

6.2.6.1 Gateway Screening for Reliability

Key Learnings

Issue:

Service reliability and security can be affected by inter-network signaling traffic that does not conform to normal operational procedures creating a need for improved network interconnect robustness.

Background:

There is a need to enhance intercarrier security beyond the ANSI Gateway specifications to defend against abnormal signaling network operation between interconnecting networks. Examples include protecting service provider networks from inter-network propagation of bad messages, sabotage, and congestion.

Enhancements to Gateway screening functionality may be required to provide:

- defenses against damage from receiving from connected networks all possible values in variable protocol fields, whether or not they are currently valid;
- defenses against unresponsiveness by connecting networks to congestion indications;
- defenses against oscillating signaling links due to interconnecting networks;
- defenses against connecting network "black-holing" signaling messages;
- defenses against long correlated message failures; and
- defenses against excessive long correlated message traffic.

A number of signaling network elements may already provide protection in some of these areas.

Recommendations

It is recommended that T1S1 should be solicited for contributions to the NIIF for formulation of Data Connection Trust Agreements (as shown in Section 6.7) and other solutions to this problem.

It is recommended that standard bodies should be requested to solicit recommendations to outline areas of improvement and provide recommendations (issue standards as required) to improve network interconnect robustness.

6.2.6.2 Looping Messages

Key Learnings

Issue:

Need the ability to guard against, detect and eliminate looping messages that may be generated when multiple carrier's networks are interconnected and routing information databases are inconsistent.

Background:

For example, the problem could arise if STPs and/or SCPs are out-of-sync regarding Global Title Translation (GTT) for a particular 10-digit number. Circular routing of GTT messages can potentially cause network reliability problems especially with an increased message traffic load resulting from the implementation of LNP. There are a number of techniques that have been or are being investigated to address this potential problem, some of which are:

- the use of a Signaling Connection Control Part (SCCP) Hop Counter to detect SCCP message looping between SS7 networks;
- the use of an SCCP Route Verification Test (SRVT) to detect data provisioning errors that could cause SCCP message looping;
- the use of an Integrated Service Digital Network User Part (ISUP) hop counter, already defined in ANSI T1.114 protocol; and
- the use of MRVT to detect data provisioning errors that could cause ISUP message looping.

Recommendations

It is recommended that T1S1 solicit contributions that fully define the looping message issue and that address a comprehensive set of functions that ensure against this reliability risk.

6.2.6.3 Signaling Link Diversity

Key Learnings

Issue:

There is an increasing need to ensure continued signaling link route diversity on all network facilities assigned to carry signaling links or link sets especially when leased facilities are utilized.

Background:

It is becoming a common practice for signaling network interconnections between service providers (*e.g.,* LECs and CLECs) to be implemented via leasing facilities from a third party. Also, when new high-speed facilities (*e.g.,* SONET facilities) replace retiring facilities it is quite possible that link diversity is compromised due to the concentration of many circuits into one high capacity facility. This makes it difficult to manage signaling link diversity. There are currently no automated services that identify when a signaling link is present in a particular facility to indicate caution is required when associated circuits are reassigned. This problem is compounded when signaling links of multiple carriers get assigned to the same facility or facility route.

Recommendations

It is recommended that a carrier's interconnection template should ensure that signaling link diversity is established and maintained, preferably by an automated process.

It is also recommended that NIIF investigate signaling link diversity issues and provide recommendations for an automated process to ensure long-term integrity of signaling link diversity.

6.2.6.4 Scheduled Maintenance

Key Learnings

Issue:

With more and more service providers interconnecting their signaling networks, performance of routine scheduled maintenance functions may have undesirable affects on adjacent networks especially if effective coordination of maintenance windows is not enforced.

Background:

In some cases normal network redundancy may temporarily be unavailable during maintenance windows so that maintenance functions can be performed on associated equipment. If an interconnecting network were unaware of such conditions network reliability could be affected.

Recommendations
It is recommended that interconnected service providers establish and maintain coordination administrators who ensure, by implementing defined notification rules, maintenance activities by both parties do not jeopardize signaling network reliability.

It is also recommended that the administration of maintenance activities that affect two or more service providers should follow rules negotiated before service initiation and incorporated within bilateral service agreements.

6.2.6.5 Change Management

Key Learnings
Issue:
The Signaling Network changes on a regular basis due to a number of factors. With increased interconnection of the signaling network, an increased number of change notifications to coordinated database elements will be required. This process needs to be error free or services will be misdirected and the network could become unstable.

Background:
Normal growth, GTT data base changes, SCP data base changes, new service introduction and traffic engineering initiatives are a few of the events that traditionally cause change in the signaling network data. The impending surge in database activity related to LNP requires new focused attention from industry to ensure signaling network reliability. LNP database entries, reflecting ported subscriber numbers, are required in multiple databases contained in multiple service networks. Non-alignment of this data due to distribution timing issues, network faults or other reasons can have a negative effect on overall network performance that may affect subscriber service performance associated with multiple carriers. Looping signaling messages that result from non-aligned data may saturate signaling links between STPs and between STPs and SCPs, preventing other call associated signaling traffic flows. Coordination efforts between carriers that ensure consistency of signaling network information is required to maintain service reliability.

Work is being performed in industry to address a number of the issues related to the maintenance of LNP databases. The Local Number Portability Administration within NANC is addressing the issues related to a nationwide system of regional SMSs and the distribution of ported numbers to the number portability databases.

Recommendations
It is recommended that NANC continue to address issues related to local number portability databases, ensuring timely number distribution and ensuring data consistency across all associated LNP databases.

It is recommended that T1S1 address signaling network architectural issues related to the query of the LNP databases to reduce the instance of looping messages due to inconsistent data in

multiple databases and to minimize or eliminate any adverse signaling network traffic that would cause reliability risks.

6.3 PERFORMANCE MONITORING

With a high level of "nondiscriminatory accessibility by the broadest number of users and vendors," it will be a challenge to maintain an acceptable level of performance for the overall public switched network infrastructure, as well as its individual subsets or components. The public, in general, as users of telecommunications services, and the FCC in particular need a method of ensuring that the overall health of the network is maintained while opportunities for interoperability and enhanced market competition are being facilitated. Service providers are also concerned that the interfaces or Gateways with new entrants to the market will be established and maintained for optimum performance characteristics. These interfaces and Gateways will be designed to protect the network assets of both the new and incumbent carriers and should include performance monitoring features.

Performance monitoring is designed to measure the overall quality of service through the use of monitored parameters in order to detect any degradation from a set of agreed upon service measures. Performance monitoring measures vary depending on the expectations of each group of participants in the telecommunications arena. There are also differences in the responsibilities and obligations of each group. This section addresses the expectations of each group related to performance, the responsibilities and obligations that should be met, and the performance measuring capabilities, techniques and processes that may be employed to ensure service levels.

Performance monitoring is an evolving capability that will require work in standards, forums, and other industry groups to define the measures and reporting structure for an expanded, competitive telecommunications industry. Monitoring of the overall health of the industry will remain a responsibility of the FCC and regulatory agencies within their domains of responsibility. Recommendations included in this section address the measures that should be developed and the group(s) deemed best able to define them. Of paramount importance is the participation of all segments of the telecommunications industry; cable, wireless, voice, Internet, video and so on, in the establishment of the performance monitoring objectives, and measures.

6.3.1 Different Perspectives (Expectations) of Performance Monitoring

All participants in the telecommunications arena, including consumers, service providers, equipment vendors, and regulators, have an interest in determining the effectiveness of network interoperability. Their interests are from different perspectives with different expectations of performance and different needs for performance monitoring and performance measures. A set of performance monitoring measures and reporting requirements should meet the needs of the various participants. To define a robust set of measures and reporting requirements, relevant categories of services should be established.

In establishing the service categories, three fundamental perspectives provide a high-level division of the different needs:

a) FCC and Regulators - measures that assess the overall health of the nation's telecommunications infrastructure and provide reliability assurances.

b) Service Providers - measures that give insight into the effectiveness of technology interfaces and promised capabilities and can be analyzed to assist in determining if significant problems exist; their root causes, and what corrective/protective actions can be taken.

c) Service Consumers - measures that provide an "end user" visibility into the effectiveness of service delivery from various service providers.

These three perspectives must be applied to establish performance objectives across the range of different telecommunications services, including voice, data, and video, and encompass the incumbent service providers as well as the new entrants.

Background:

a) The expectations of the FCC and other regulatory organizations should include the ability to determine the health of the current telecommunications infrastructure and the resulting impacts of directives or legislative requirements that are imposed on the networks or network subsets. Additionally, the impacts of industry changes to the networks due to market forces need to be monitored to ensure an overall infrastructure degradation does not occur. The benefits of nondiscriminatory access, competition, and technological innovation should not become outweighed by a significant decline in overall network reliability. Appropriate measures will provide a continuing report on the overall performance of the network, and establish a benchmark for future assessments and trouble analysis.

b) The Service Provider perspective of interoperability performance monitoring encompasses the needs of both a seller and a buyer of network asset use. As a seller, the Industry Provider wants to make sure that his assets provide the utility promised and that they are not being abused. As a buyer, the Industry Provider wants to make sure he is getting the asset use promised and paid for. In both cases, the Service Provider may be viewed as a trusted party who expects to be interoperating with a trusted party. The appropriate interoperability

performance measures will give insight into the effectiveness of the technology interface between the two parties and the delivery of capabilities as promised. The measures will provide the data that can be analyzed to assist in determining if significant problems exist and their root causes.

c) The expectations of service consumers range from the individual person who requires telecommunications service for social, business and personal applications, to the U.S. Government requirement for critical National Security and Emergency Preparedness (NS/EP) purposes. The individual consumer expects sufficient information and performance measures that can be used to make intelligent choices between competing services, capabilities, and products. Agencies, departments, and organizations of the Federal government with NS/EP missions expect adequate communications capabilities to allow for prompt management actions and emergency response activities during disasters or other national emergencies.

Key Learnings

To determine the service levels that should be established to meet the participant expectations and needs, the following considerations should be used:

a) The FCC perspective is reflected in the charters for NRC I, NRC II, and NRIC, all of which relate to the health of the public switched network. The purpose was to provide recommendations both for the FCC and for the telecommunications industry that, when implemented, will:

- "help prevent public telephone network outages from occurring."
- "continue to keep the public switched network reliable and, at the same time, accomplish increased interconnection and introduce major new technologies into the network."
- "assure optimal reliability and interoperability of, and accessibility and interconnectivity to, the public telecommunications networks."

The first efforts determined and analyzed the root causes of outages and provided recommendations and templates for corrective actions. The current focus is in maintaining reliability while removing the barriers to increased interoperability.

b) Service Providers share the common perspective that value to the consumer is highly dependent on interoperability transparency. For this reason it is particularly important that the measures applied in interoperability monitoring be mutually understood and agreed upon as the means by which to evaluate compliance with service requirement specifications and for service trouble reporting and resolution. Such understanding and agreement is necessary to enable expeditious resolution of troubles without wasting time and resources seeking to understand the other party's cause for concern or disputing the relevance of their measures.

With the unbundling of the network, interoperability may occur at many points over several levels. Each level could have its own set of measures. For example, interoperability may occur at:

- a physical level with assignment of certain seller's cable pairs in a cable for termination on a buyer's co-resident switch, with interoperability performance monitoring and measurement agreements needed as to the level of signal permitted on the wire pairs and the rate of pair outages and repair times;
- a logical level where the seller provides certain channels in an interoffice transmission multiplexer to interconnect two buyer's switches, with interoperability performance monitoring and measurement agreements on the transmission parameters, outages, and repair times;
- a service level where telephone number translations are provided by the seller to enable the buyer to properly route a call, with interoperability performance monitoring and measurement agreements on transaction capacity, response time, and resource availability; and
- an operations support level where the seller provides the buyer the means to enter new numbers for translation in the seller's database used by the seller to provide the buyer a number translation service, with performance monitoring and measurements agreements on frequency of database updates, transaction capacity, and resource availability.

Although there may be many interconnection agreements (sometimes in the form of handbooks) defining specific measures and monitoring requirements, the most common requirements should be established through the process of industry standards. At a minimum, such agreements should cover:

- definition of the measures to be applied to establish delivery of the agreed upon interoperable service;
- specification of measure values establishing the tolerance range for service acceptability;
- mechanisms to be employed to monitor interoperability, including frequency and duration of monitoring, if not continuous, and the methodology to translate monitoring results into the agreed upon measures; and
- responsibilities and obligations for reporting out-of-tolerance conditions and the restoration time.

Definitions of the measures and the methods for translating raw monitoring data into the measures are expected to be the domain of standards. Specification of measure values for specific services and responsibilities and obligations for reporting and restoration are expected to be the domain of business agreements, but with industry coordination of common values needed to facilitate universal service.

c) The Service Consumer perspective is that of a buyer who has a general understanding of the desired service and features and an expectation that the service will be provided without hidden complications. Unlike the Service Provider, the Service Consumer is not expected to be a technically sophisticated party to the transaction, and trust is generally limited to the terms of the transaction. In making his choice of service provider, the Service Consumer needs measures that provide an "end user" visibility into the effectiveness of service delivery.

Interoperability measures for the Service Consumer enable the evaluation of alternative service providers. Such measures should include:

- Mistreated Calls - the number of complaints per thousand subscribers of calls that were not delivered to the proper destination (*e.g.,* because the service provider had not updated his switches to reflect the opening of a new area code in an interconnected network, because he failed to properly route a ported number, *etc.*);

- Service Completeness - the number of complaints per thousand subscribers of requested service access arrangements that were not available (*e.g.,* inability to get roaming service because of lack of interoperability arrangement);

- Service Timeliness - the average time to complete requested arrangements for access to third-party services through interoperation; and

- Billing Clarity and Accuracy - the average number of complaints and queries per thousand subscribers regarding billing accuracy or understanding.

At the other end of the Service Consumer spectrum is the Federal government with a thorough understanding of the infrastructure, its components, and technologies associated with new capabilities and services. In general there is an Industry/Government partnership in developing, testing, and implementing new technologies to meet the most critical requirements. In addition to the measures noted above, advanced requirements may require measures in the following areas:

- Priority Recognition - the ability to successfully recognize a NS/EP call per ANSI T1.631-1993, High Probability of Completion (HPC) Network Capability; and

- Priority Treatment - the ability to successfully route a NS/EP call around areas of congestion or network damage, and the ability to exempt these calls from restrictive management controls.

As with Service Provider measures, it is important that the Service Consumer measures be well defined and supported with specifications of how monitoring is to be conducted to collect performance data and the methods by which performance data are translated into the specific measures. The source of this information should be publicly available periodicals, consumer

organizations, and industry associations, with umbrella oversight by the FCC for violations with significant community impact.

Recommendations

The broad spectrum of services should be categorized by T1A1 into subsets for which interoperability performance measures can be specified that are reasonable and recognizable to the participants.

- From the FCC perspective, the categorizations should be such that the following can be identified; major outages of service, and deterioration in the overall service levels of the industry.

- From the Service Provider perspective, such categorizations for use in negotiating their interoperability arrangements will naturally evolve as part of the standards process.

- From the Service Consumer perspective, such categorizations present a new level of challenge. The categorizations and measures, to be most effective, require the service providers' commitment to the monitoring and reporting of performance. Such commitments may evolve through consumer advocacy groups.

The first set of services that should be considered are those that impact the greatest number of customers. In the past these types of measures have largely focused on voice services supplied by traditional telecommunications providers. With the increase in cellular, data, and video communications, the service subset should now be expanded to include facilities such as signaling interconnection Gateways and backbone facilities for all providers, including those facilities that support the cable TV industry and wireless service providers. Both frequency of failure and length of failure indices should be established. Reporting of these indices should be supported by performance monitoring data supplied by the appropriate communications components.

It is recommended that standard bodies such as T1A1 should establish the services to be measured and determine how they should be measured. Industry participation by all service providers and equipment vendors should be encouraged by the FCC.

6.3.2 Responsibilities/Obligations of Industry Participants

As the networks and network subsets become open to an increased number of new entrants, the responsibilities and obligations of these new entrants, incumbent service providers, regulatory bodies, standards groups, and industry associations must be expanded to accommodate the changes. The same level of trusted relationships as currently exists must be achieved within the industry, and respected memberships established in industry associations, if new entrants are going to successfully interoperate with the incumbent carriers. Additionally, regulators,

standards bodies, and advisory groups should not back away from promoting, defining, and improving levels of performance and reliability that correspond to user expectations noted above.

Background:
Following divestiture, regional Bell operating companies successfully separated themselves from the single parent company and established the necessary trusted relationships to ensure a high level of performance and reliability was maintained in the network infrastructure. Through forming of industry associations and standards bodies, and carrier-to-carrier negotiations, each of the divested parties has grown into a vital element of the infrastructure. This same degree of growth and involvement will be expected from the new entrants as they begin to interoperate with the incumbent carriers. Likewise, the existing industry associations, standards bodies, and regulatory groups must evolve to extend memberships, benefits, and coverage to the new industry partners.

Key Learnings
At the most basic level, new entrant interoperability is achieved through carrier-to-carrier or service-provider-to-service-provider negotiations. At that level there is the mutual responsibility to negotiate in good faith, identifying the specific service expectations and performance measurement points that can confirm that obligations are being met. The Network Interconnection Bilateral Agreement and Network Interface Specification Template developed for NRC II, and updated for this NRIC, provide a list of items to be covered by these negotiations. As multiple interconnection agreements are reached, it would be the responsibility of existing industry associations and standards bodies such as the Network Interoperability and Interconnection Forum (NIIF) to look for commonality in the agreement and to establish handbooks and eventually standards that identify the performance parameters that should be applied to similar interconnection agreements. In all cases, the existing agreements should clearly identify the actions that may be taken by either party if performance thresholds are exceeded. If disputes occur after an agreement is in place, industry associations or forums should be included in a process to settle the dispute before a breakdown occurs, agreements are terminated, or services cut off. The FCC or other regulatory bodies should have the responsibility to monitor the process of dispute resolution to ensure the health of the overall network is not affected. Depending on the nature of the service and the disputed performance objective, groups such as ATIS, Network Security Information Exchange (NSIE), National Security Telecommunications Advisory Council (NSTAC), NIIF, Telecommunications Industry Association (TIA), United States Telephone Association (USTA), or NSCA may be involved.

Industry journals and consumer interest publications may also contribute to this process. As agreements are reached that result in new business opportunities and competitive services, it is the responsibility of these journals to report on these events. Likewise, if the performance measures in the agreements cause a negative result on the overall health of the communications infrastructure, higher consumer costs, or degradation of service alternatives, they also have the responsibility to report those issues.

Recommendations

Specific agreements between service providers will determine the continuance of a trusted relationship between industry partners. A checklist of items to ensure service levels are maintained that can be included in the agreements between industry partners is available in the interoperability templates developed for NRC II and updated for NRIC. Performance monitoring parameters should be identified for critical items that impact the ability of interconnecting parties to complete their normal business activity.

Performance monitoring will also be used to monitor compliance with items mandated by regulatory bodies such as access to operational capabilities. Performance measures for operational access should include measurements designed to monitor occurrences of system access congestion including root cause analysis.

6.3.3 Required and Desired Performance Monitoring Capabilities

Whether the network is owned, operated, and maintained by a single company, a handful of regional companies, or a larger number of interoperating, functionally oriented service providers, the required and desired performance expectations and objectives remain basically the same. The methods of measuring performance vary with new entrants, changes in the access model due to unbundling and interconnection, and technological innovations. The capabilities required to measure performance have grown with expansion of the industry and should be expanded to include all entrants and technologies. Definition of these capabilities will be assisted as new industry partnerships are formed with companies and service providers that may be competitors in the same marketplace. The successful transition to a network infrastructure with a high level of nondiscriminatory access must include the sharing of these performance monitoring capabilities.

Background:

The performance monitoring capabilities of the network and network subsets do not need to undergo a significant change due to the increased number of new entrants. These capabilities must be shared, as they are already shared within each company's organizational structure. Trusted partnerships that must be formed and mutual respect for each others' goals will determine the degree to which performance capabilities, data, and measures are shared. Likewise, the existing performance monitoring requirements of the FCC and other regulatory bodies provide a sound basis for including new entrants without diluting the overall health of the communications infrastructure. New performance measures will be required to monitor interoperability at interfaces and Gateways between vendors, and to monitor new technologies that carry telecommunication services.

Key Learnings

The exchange of performance data between service providers allows service providers to better assess the end-to-end impact of outages on end-users and determine effective means for improving performance. It also allows service providers to take immediate steps to protect the networks and customers' interests if established thresholds are exceeded. Some of the performance data that may be exchanged between carriers include the following:

- circuit availability for various service types,
- mean-time to repair (MTTR),
- percent greater than standard MTTR,
- percent troubles reported but found in other carrier's or customer's system,
- repeat troubles,
- per cent service delivered compared to requested due date,
- failure after installation (*e.g.*, within 30 days of turn-on),
- blocked calls, and
- network outages per major event and duration of outage.

Additional performance data previously kept internal to each service provider may now have to be shared as networks become unbundled. Example measures include:

- circuit and system availability,
- transmission measures,
- utilization (trunks, ports and spans),
- trouble sources and closures,
- trouble reports per call attempt and per circuit,
- blocked calls per outage, and
- call completion ratio.

Performance measures for voiceband services in the wireline segment of the telecommunications industry have been developed. For example, T1A1.2 has developed a generic outage index methodology that does not depend on the network technology [T1 TR No. 24]. This work included an appendix on U.S. Government user expectations and an appendix on tolerance categories for restoration times.

T1A1.2 is in the process of drafting a Supplement to this methodology to address each industry segment individually and to address the need to include voiceband services provided by the cellular, satellite and cable TV industries. It is expected that this supplement will be completed during the summer of 1997.

In addition to this work on a generic outage methodology, T1A1.2 completed a technical report on the analysis of FCC-Reportable service outage data [T1 TR No. 42]. An outage index was developed that combined the services affected, duration, and magnitude (number of customers affected). Various properties believed to be essential for such an index included:

- weight given to the relative importance of outages for different services,
- the ability to aggregate outage data through the index to allow comparisons over time, and
- weight given to the impact of small and large outages, as perceived by the public.

Calculation methods, service outage examples, and trend analysis techniques were provided. These methods have been applied by the Network Reliability Steering Committee (NRSC) in its analyses of outage reports for several years. These techniques were also developed to be applicable within private networks and for extension to other segments of the telecommunications industry. Related work by T1 committees, the International Telecommunication Union (ITU), the National Communications System (NCS) and NCCS is outlined in T1 TR No. 42.

Recommendations

All interconnecting parties (established and new) should specify in their interconnection agreements the parameters to be monitored to maintain normal business activity and pre-agree to the triggers and actions to be taken if those parameters go out of bounds.

Work in existing standards bodies and industry forums on network reliability performance measures should be extended to facilitate its application in new segments of the voiceband services telecommunications industry (cellular, satellite, cable TV, CLECs and ILECs). This work will adapt measures such as the outage index of existing measures to clarify their application to these other segments and also to suggest ways in which selective exchange of these measures can better assess the impact of outages within one segment on the other segments it is connected to.

The existing templates for reliability and interconnection criteria [NRC II template] and interconnection templates [Network Operations Forum (NOF) draft handbook for interconnection between LECS] should continue to be refined and updated to reflect the rapidly evolving telecommunications environment. These changes will facilitate highly reliable customer services in future, more fully interconnected networks.

Based on the recommendations made earlier in this section, it is expected that T1A1.2 and NIIF would define specific service subsets and thresholds for use in performance monitoring. These performance monitoring items would apply across the industry. Once these service subsets and thresholds are identified, ATIS NRSC should then recommend specific performance monitoring items that could be reported by the industry and formally tracked by the FCC and other regulatory agencies.

6.4 SECURITY OF THE PUBLIC TELECOMMUNICATIONS NETWORK

6.4.1 Issue*:*

Section 251(C) of the Telecommunications Act of 1996 requires Local Exchange Carriers (LECs) to provide nondiscriminatory interconnection and "unbundled" network access to any requesting telecommunications carrier "at any technically feasible point." The Act also directs the FCC to "establish procedures for the Commission oversight of coordinated network planning by telecommunications carriers and other providers of telecommunications services for the effective and efficient interconnection of public telecommunications networks".

The FCC in turn identified a minimum set of "technically feasible" points of interconnection at local and tandem switches and also provided for access to unbundled network elements.

The intent of Section 256 of the Act is to ensure the development of standards that promote access to public telecommunications networks providing telecommunications service. Its purpose is to promote nondiscriminatory accessibility by the broadest number of users and vendors of communications products and services to public telecommunications networks, through coordinated public telecommunications network planning and design and **public telecommunications network interconnectivity,** and interconnectivity of devices and to ensure the ability of users and information providers to seamlessly and transparently transmit and receive information between and across telecommunications networks.

As defined in Section 256 of the Act, the term **'public telecommunications network interconnectivity'** means the ability of two or more public telecommunications networks used to provide telecommunications service to communicate and exchange information **without degeneration**, and to interact in concert with one another.

Although the Act does not specifically mention or address Public Switched Network (PSN) security, the FCC in its First Report and Order issued language to reflect its sensitivity as to what may arguably be considered technically infeasible due to the potential for such degeneration through degradation of security or reliability.

As part of its deliberations, Focus Group 1 was tasked to specifically consider whether the templates developed by the Interconnection Focus Group and the New Technologies Focus Group of NRC II are sufficient to meet the requirements of the statute. The group was asked to focus particular attention on security issues. If Focus Group 1 determined that the existing templates and guidelines are not adequate, then Focus Group 1 was expected to develop or recommend the development of additional, or more refined templates and practices.

Given the degree of trust required to provide the level of accessibility demanded by the Act, it will be a challenge to maintain an acceptable level of security and reliability for the public switched network infrastructure. However, the challenge can be met if industry meets the

increased risks with increased awareness and uses available strategies, tools, techniques and testing for security and reliability.

While much has been accomplished by the industry to address the issue of network security within the PSN, with few exceptions the countermeasures set in place were based upon a flat single service provider perspective.

The intent of NRIC Focus Group 1, Task Group 3 is to present an offsetting set of references and planning strategies to offset risks that may arise as a result of the increased interconnection, unbundling and extended networking mandated by the Act.

6.4.2 Background on Security

The National Research Council in their 1989 report entitled *The Growing Vulnerability of the Public Switched Network: Security Implications for National Security Preparedness* predicted that "were all private and public networks to be fully interconnected and employ common software, the entire network could be at risk if a hostile user were to find an exploitable flaw in system software." While the degree to which all public and private networks have interconnected and employ common software may be debated, it is certain that the growth of and connectivity to public data networks such as X.25, Frame Relay and the Internet have exacerbated the vulnerability of the of the Public Telephone Network (PTN). During the last decade, the nation has experienced numerous cases of computer related crimes, by individuals and groups , with the requisite **SKAM** (**S**kills, **K**nowledge, **A**ccess and **M**otive) acting on an increasing number of exploitable vulnerabilities. As the information superhighway has evolved into a user friendly, open, globally connected, nomadic, anywhere, anytime, any-media, full service communications network of networks, so have the systems used to Operate, Administer, Maintain and Provision (OAM&P) the PTN. The deregulation of the industry, absent security standards and solutions for managing risk in an open competitive unbundled Telecommunications environment, may drive enormous holes in existing security mechanisms and access controls to the executable code of the public network building blocks, network elements, operations systems and data communications networks.

While there is a rich, if not open, history associated with the security exposure and risk management of the PTN, the security issues arising from the interconnection of telecommunications networks and systems over the last decade is without precedent. In the first half of the last decade, the level of resources needed to compromise the primary security mechanisms to protect the public telecommunications network fell significantly largely due to increased network interconnection and deficiencies in three major areas: security policy, human factors and technology. Through industry and government efforts to understand and address the PTN three dimensional security problem referenced above, much success has been achieved to help prevent, contain and recover from security threats such as hackers, disgruntled insiders and economic espionage agents. One of the lessons learned is the need to address security over the life cycle of the technology platform.

Unlike the Internet and its World Wide Web, notwithstanding the massive Toll Fraud Problem, the PTN has not recognized significant security exposure related to the exploitation and corruption of vulnerable computer and networking technology. This is not to say that there have not been serious incidents nor that the PTN is secure due to its technology base alone, since much of the same technology utilized within the vulnerable Internet is integrated into PTN OAM&P platforms and networking. The two factors that have kept the PTN reasonably secure, even with the massive complexity of the Advanced Intelligent Network and the 800 Portable Number Plan, are the access control mechanisms and security baselines used by most carriers today to allow access only to authorized individuals and processes with a valid business need for access. It is therefore no surprise that the vulnerability of the Public Telecommunications Network could be significantly exacerbated by the increased access, and the abuse that such access may afford, to network elements, operations support systems, data bases and signaling mandated by the Act.

While sophisticated test plans have been developed and implemented within the industry, by Bellcore's Technical Analysis and Auditing Programs, to provide a comprehensive framework for the interconnection of common channel signaling networks and the interconnectivity of associated devices, little has been done to afford for effective testing of security within and across evolving PTN network boundaries and interfaces. Today's networked electronic environment provides many advantages for moving information, money, energy, data, designs, *etc.*, literally at the speed of light, from one point to another. Unfortunately, this same environment provides far too many opportunities for the unauthorized access, disclosure, modification, disruption, destruction or theft of this same information.

In their 1994 report[38] the National Communications System (NCS) found that:

> *The threat to the Public Switched Network, due to advances in technology and sophistication of intruders, is significant. The results of the electronic intrusions may have serious ramifications for both the Public Switched Network and the National Security and Emergency Preparedness telecommunications that rely upon it.*

In addition to the increased PSN vulnerabilities and dependencies, there has been a significant increase in the sophistication and abuser friendly nature of intrusion tools, techniques, tutorials and software based burglar tools available on the World Wide Web.

During the five-year period from 1987 to 1991, the levels of resources needed to compromise the primary security mechanisms that protect the public switched network and the packet switched networks, such as X.25, fell significantly due to the growing sophistication of both intruders and the technological tools they use. Forensic analysis of hundreds of incidents, over the past two decades reveals more than a dozen root causes of intrusion. During the past 10 years, the number of compromised systems, routers, networks, and services supporting the growing information superhighway have escalated, potentially affecting tens of thousands of nodes. It has become

[38] *: OMNCS, "Electronic Intrusion Threat to NSEP Telecommunications" Sept. 30, 1994*

increasingly clear that networked systems are more vulnerable to attacks through interconnections with other networks. Such attacks always involve either entirely unauthorized persons or persons who exceed the level of authorization they do have. They act on exploitable vulnerabilities using their Skills, Knowledge, Access, and Motive to exploit.

Like the Internet Worm incident back in November 1988, which exploited known holes in UNIX and VAX computer systems, intrusions into the cyberspace of public switched networks also exploit known holes or bugs. Computer intruders, whether inside or outside an organization, can easily acquire the technical skills and knowledge to manipulate the PSN and the content riding within the PSN. Easily accessible publications such as 2600, The Hacker Quarterly and Phrack Magazine provide technical descriptions and generally accurate instructions for exploiting the vulnerabilities of the PSN and network elements, including digital switches. Intruders often use telephone-fraud-type methods to avoid telecommunications costs and records. Increased levels of system complexity and decreased levels of training and knowledge at the system administrator level combine to create a situation susceptible to exploitation by individuals inside and outside the system. Given this information, it would appear the only practical solution to PSN security is to *mediate access and close exploitable vulnerabilities* while new firewall standards, technology and platforms are being deployed from the network research and standards community.

6.4.3 Problem Statement and Key Learning Issues to be addressed:

A survey conducted by Focus Group 1 identified over two hundred perceived barriers to interconnection. Of those perceived barriers, approximately 15 % are information protection or network security related. Technical Analysis of the security related barriers by the Focus Group 1 Operations Task Group and draft input from the NSTAC Network Security Group, looking at the security implications of the Act on National Security and Emergency Preparedness, developed the following risk management security issues or concerns:

1. Increased number of access points and collocation will likely decrease core infrastructure diversity and increase single points of failure
2. Increased number of interconnected service providers with inferred trust relationships will degrade overall security and network integrity
3. Embedded Operations Channels of advanced Signaling and Transport Protocols (*e.g.*, SONET DCC, ATM OAM Cells, SS7 Network Management Messages) give virtually unlimited access to everything and everyone connected to them, given the current state of security standards and practices in such advanced technologies.
4. Increased number of persons and processes with privilege will present major risk challenges
5. Insecure Internet and Intranet technology used for interconnection access to Network Operations and Signaling Systems will provide unintentional back doors to PSN mission critical systems, protocols and information
6. Perceived lack of Regulatory, Legal or Competitive motivation to invest in security safeguards will increase risks to the PSN

7. Lack of requirements, fidelity bonds, background checks, or other fiduciary requirements, given the Communications Assistance for Law Enforcement Act (CALEA) control requirements of Section 229 of the Act, will increase risk to the PSN.

The Focus Group 1 Task Group 3, Security SubGroup first sought to determine what the engineering or other technical security barriers are to the interconnection and accessibility of networks, both for networks and for network services. It then reviewed the prior work of the Network Reliability Council from the perspective of the statute and determined whether those findings had adequately identified security barriers and safeguards to the interconnection and accessibility of networks and network services.

While existing security mechanisms[39] address many of the security issues from a single local exchange service provider standpoint, there is a need for a standard defining baseline security requirements for interconnected data communication networks and gateways that support Public Switched Network interconnection and partitioned access. The perceived barriers and security issues related to signaling[40] are addressed to some degree by existing bilateral agreements, best practices, standards and NRC templates. Section 9 of the NOF Reference Document contains the Security Base Guideline for Interconnected SS7 networks.

Many of the recommendations contained within the NRC II, Increased Interconnection Task Group II Report, dated January 14, 1996, reflect and support the expansion of solutions to security and reliability risks in an open-market, interconnected world.

[39] Bellcore Generic Requirements, National Institute of Science and Technology Standards and ANSI T1-233, 234 and 252

[40] Security of the signaling network in a multi-carrier environment ensures the integrity of all access points to the signaling network including signaling links, embedded operations channels, and other operations systems (OS) access interfaces.

6.4.4 Findings and Recommendations

Within service contracts today between telecommunications carriers, bilateral agreements on interconnection and unbundling of services are reached through the utilization of interconnection templates, which include NOF Reference Document checkpoints together with established and proven standards such as ANSI T1-252, 233 and 243. Existing measures, templates, standards and reports support but do not adequately address findings and recommendations to avoid security barriers to network interconnection, specifically Signaling and unmediated Operations Support Systems access, at this time. Specific recommendations to address the security issues related to Signaling and Operations Systems Access are contained in Sections 6.1.1.4 and 6.2.5 of this report.

1. Finding:

Existing measures, templates, standards and reports support but do not adequately address findings and recommendations to avoid security barriers to network interconnection, specifically Signaling and unmediated Operations Support Systems access, at this time.

Recommendation: It is recommended that the NIIF expand the Bilateral Interconnection Template (NIIF Issue 0014) to reflect the Security applicable best practices, standards (Committee T1), base guidelines (*e.g.,* NIIF Network Operations Document Section 9) and Data Connection Trust Agreements (See Operations Section 6.7.4 Sample Data Connection Agreements, page 65). It is further recommended that the ATIS Network Reliability Steering Committee expand the Outage Reporting Cause Code fields better capture security related agents and problems.

2. Finding:

SS7 Gateway screening (firewall) capabilities are neither adequate nor reliable to address a sophisticated attack on the PSN, PSN providers or PSN users.

Recommendation: It is recommended that the NIIF expand its reliability efforts to address gateway security screening against harmful messages and spoofing (deliberate insertion of false or misleading messages or message content). It is also recommended that the appropriate standards groups, service providers and equipment suppliers be strongly encouraged to apply the recommendations from NRC II as they relate to security issues with particular emphasis on firewalls, harmful code detection and mediated access.

3. Finding:

There is increased potential exposure to intrusion brought about by procedural errors affecting security during CLEC implementation of various mandates within the Act *i.e.,* Local Number Portability, combined with the possible exploitation of these windows of vulnerability.

Recommendation: It is recommended that affected carriers and vendors reinforce their defensive, detective and reactive fraud detection and network security capabilities and resources to deal with the increased risk and provide additional training, tools and participation in at least two industry fora such as the ATIS Toll Fraud Prevention Committee, the NSTAC Network Security Information Exchange and the Forum for Incident Response and Security Teams (FIRST).

4. Finding:

There is no certifying authority or body to effectively test for security conformance to the various standards, or working agreements. At best, bilateral agreements may contain right-to-audit provisions but generally do not address trust worthy data connection agreements or SS7 firewalls.

Recommendation: It is recommended that Service Providers and equipment suppliers test for security conformance. Every effort should be made to see if security can be included in the interoperability and stress testing done by the NTC/IITC.

5. Finding:

Additional security efforts are necessary.

Recommendation: It is recommended that ATIS expand the charter of the Toll Fraud Prevention Committee (TFPC) to address network security. It is also recommended that the industry support ATIS and actively participate in the expansion of the TFPC.

6.4.5 Summary:

Increased security and reliability risks will arise from the Telecommunications Act's mandated interconnection and unbundling of key elements of the PSN infrastructure. To counter that trend, the industry and the Commission will need to pay continuing attention to security risks as they continue to develop in the new environment. Special attention should be paid to the following areas:

- ***Standards*** *e.g., ATIS NIIF (NOF) Reference Document Section III, Subsection 9, Network Security Base Guideline, and ANSI T1 233-1993, ANSI T1.243-1995 and ANSI T1.252-1996 Telecommunications OAM&P Security Framework, Baseline Security Requirements for Telecommunications Management Networks (TMN) and TMN Directory**, and** additional T1 standards for partitioned access control and firewall within a TMN Gateway environment*
- **Access Control, and Audits:** *e.g., Access Control Lists and Data Connection Agreements to facilitate secure open market electronic commerce*
- **F*irewalls*** *e.g., STP Gateway Screening, Near Network Element Concept, Closed-User Groups, Proxy Servers, Internet Firewalls, Frame Relay Firewalls and Encryption, Connectionless Security Features of SMDS, etc.*
- **A*uthentication*** *e.g., Strong, Robust,, User Friendly, Open Standards Based and Manageable like RADIUS*
- **R*eporting*** *of security related reliability impacting incidents and outages.*
- **I*ntrusion Detection*** *and containment through cooperating security points of contact referral and enforcement of the Data Connection Agreement(s)*

6.4.6 References*:*

- *National Information Infrastructure (NII) Risk Assessment : A Nation's Information at Risk,* Prepared by the Reliability and Vulnerability Working Group, February 29, 1996
- *Alliance for Telecommunications Industry Solutions (ATIS), Network Operations Forum Reference (NOF) Document Issue 11 and later, Section II, Installation and Maintenance Responsibilities, SS7 Link and Trunk Installation and Maintenance Access Service, Subsection 9, SS7 Network Security Base Guidelines.*
- *Network Security Standards For Public Switched Network: Issues and Recommendations,* National Communications System, The President's National Security Telecommunications Advisory Committee Network Security Standards Oversight Group, October 1994
- *Final Report of the Common Channel Signaling (CCS) Task Force.* The President's National Security Telecommunications Advisory Committee, January, 1994
- *Operations Technology Generic Requirements (OTGR): Network Element (NE) Memory Administration - NE Operations Security,* TR-TSY-000815, Bellcore, Section 2.3 of the OTGR
- *Generic Requirements For Data Communication Networks,* TR-STS-0001332, Bellcore

- *American National Standard for Telecommunications - Operations, Administration, Maintenance and Provisioning (OAM&P) - Security for the Telecommunications Management Network (TMN) Directory*, ANSI T1.252-1996, American National Standards Institute
- *American National Standard for Telecommunications - Operations, Administration, Maintenance and Provisioning (OAM&P) - Security Framework for Telecommunications Management Network (TMN) Interfaces,* ANSI T1.233-1993, American National Standards Institute
- *American National Standard for Telecommunications - Operations, Administration, Maintenance and Provisioning (OAM&P) - Baseline Security Requirements for Telecommunications Management Network (TMN) Interfaces*, ANSI T1.243-1993, American National Standards Institute
- *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications Awareness Document, Office of the Manager – National Communications System (NCS),* Second Edition, December 1994
- *Masters of Deception: The Gang That Ruled Cyberspace,* By Michelle Slatalla and Joshua Quittner, HarperCollins Publishers
- *Recipe For Hacker Heartburn*, ASIS, Security Management Magazine, January 1995
- *Securing A Global Village: Security Baselines For Interconnected SS7 Networks, Kluepfel H.M.* IEEE Communications Magazine, September 1994
- IEEE Communications Magazine, September 1994
- *Proposed IETF Standard (Radius) to ease a variety of Remote Access Concerns*, Network World, August 14, 1996
- *National INFOSEC Technical Baseline: FIREWALLS, Lawrence Livermore National Laboratory, Sandia National Laboratories April, 1997,* http://doe-is.llnl.gov/nitb/docs/fw970401.html

6.5 INTEROPERABILITY

Background:

Today's telecommunications marketplace is characterized by increasingly complex combinations of products and services from a variety of service providers and vendors. It is driven by sophisticated, quality-conscious consumers. Services, as perceived by the end-user, are in fact provided by elaborate combinations and interactions of Customer Premises Equipment (CPE) with various Local Exchange Carrier (LEC) networks, Inter-Exchange Carrier (IEC) networks, and a wide assortment of new entrants into the marketplace. In turn, each of these networks consist of several different pieces of equipment, often from multiple vendors. As a result of the Telecommunications Act of 1996, these combinations and services will proliferate with a wide assortment of new technologies and new interconnection points.

From the customer's perspective, responsibility for combinations that do not work is often ascribed to **all** elements of the arrangement. Thus, all involved service providers and vendors have an interest in the success of the combination.

One of the key obstacles that has faced service providers in the past and will continue to confront them in the future is assuring that all involved elements are capable of communicating properly among themselves to support the requested service(s). Even when interfaces between products ("interproduct interfaces") are standard, or well documented and published ("open"), vendors typically develop unique interpretations of the interface specification. The question then becomes whether or not one vendor's interpretation interworks correctly with the other products involved in the service. In today's quality-conscious marketplace, it is critical that this question be answered **before** deploying the products/services in the field. To achieve this outcome, no substitute exists for a thorough, comprehensive test program. Mutiproduct (including multivendor) testing programs are therefore an essential element of any plan for success in the marketplace. The following sections outline key recommendations for that portion of the test program that addresses the interoperability of interconnected networks. The development of recommendations to assure the interoperability of the network elements that reside solely within a service provider's network are the responsibility of the individual service provider.

6.5.1 Funding for Industry-Wide Interoperability Testing

A prime example of a successful industry-wide interoperability testing program is the Network Testing Committee (NTC), formerly the Internetwork Interoperability Test Plan (IITP) Committee, that was instituted subsequent to major signaling outages in 1991. This arrangement has uncovered a number of SS7 problems through the years and has resulted in a sustained high degree of SS7 network reliability. NRC I recognized the value of this effort and recommended that this activity be continued on an ongoing basis. NCR II also recognized the value of interoperability testing and recommended that the scope of the NTC effort be expanded to accommodate new technologies and new interconnection points. Specifically, NCR II recommended the formation of the Internetwork Interoperability Testing Committee (IITC) under the auspices of ATIS to address ongoing industry-wide interoperability testing. In addition, NCR II recommended that industry fund this effort on a voluntary basis.

While industry has endorsed the IITC concept in principle, the actual funding mechanism has proved to be troublesome. As a result ATIS has recently formed a new IITC Steering Committee for the purpose of resolving poor industry participation and to seek best cost proposals for implementation. It is believed that the revised interoperability testing plan would include the following four basic functions:

* Determine what interoperability tests should be performed.

* Determine what test suites should be used.

* Provide test coordination

* Perform the tests.

The current IITP test coordination and hubbing function through Bellcore is supported through June of 1997. At this time, negotiations are underway to have Bellcore continue to perform the test coordination and hubbing functions through the end of 1997. The new arrangements would be operational in 1998.

A key to the success of the IITC will be the willingness of all industry participants to support the IITC operation voluntarily. The IITC Steering Committee will be working diligently to overcome previous failed efforts to have the industry keep the process funded.

Recommendations
The NRIC continues to endorse the value of industry-wide interoperability testing and funding; and encourages ATIS to accelerate the implementation of the NCR II recommendations by 3Q97.

6.5.2 Testing for Local Number Portability

A key element necessary to facilitate competition in the local telecommunications exchange is local number portability (LNP). Since LNP will be implemented throughout the nation and can impact a large number of telephone numbers, the implementation of the long-term LNP method should be field tested among carriers to assure interoperability.

The FCC in its First Report and Order in CC Docket No. 95-116 has ordered members of the Illinois Local Number Portability Workshop to a conduct a field test of the long-term portability method by August 31, 1997. The scope of these tests should be investigated by the NTC/IITC to determine their nationwide applicability. The efforts of the NTC/IITC should be coordinated with the work of the Illinois Workshop to determine whether their are any gaps. If any gaps are identified, the NTC/IITC should be asked to conduct tests that would fill these gaps. In performing the gap analysis, attention should be given to an analysis of the operation of security measures that have been established to protect access of sensitive data by unauthorized parties. In addition, consideration should be given to testing the interaction of the various databases that will be associated with LNP.

Recommendations
The NRIC recommends to ATIS that the first priority of the new NTC/IITC should be confirmation of the interoperability of LNP; making full utilization of all current field tests. In addition, NTC/IITC should investigate the interaction of the various databases that will be associated with LNP as well an assessment of the security of sensitive information and minimum performance levels.

6.5.3 Prioritization of Interoperability Tests

With increased competition there are potentially an extremely large number of interconnection combinations that could be tested. Given the limits of time and money, it would be impossible to

test all these possible combinations. A process must be developed that establishes a priority list for testing. Possible criteria to be used in establishing this list should include the area of deployment (*i.e.,* nationwide deployment versus regional deployment), schedule for deployment, and potential number of customers impacted. In addition to LNP, two other areas that should receive attention as prime candidates for interoperability testing in the near term are: i) unbundled network elements; and ii) wireline/wireless integration.

Recommendations

ATIS/IITC develops the criteria that will be used to set interoperability testing priorities. However, the NIIF should be encouraged to identify the tests that need to be performed in the next 18 months as soon as possible. Special consideration should be given to interoperability tests of unbundled network elements, wireline/wireless integration, and location oriented local number portability.

6.5.4 Coordination of Various Industry Testing Efforts

Various telecommunications industry associations, *e.g.,* IITC, CTIA's Advisory Group for Network Issues, have been identified as being actively involved in interoperability matters. ATIS' plan for the IITC calls for an IITC Oversight Group to develop the scope, charter and operating principles for the IITC. Membership is to be solicited from the Boards of various industry associations. This Group should be asked to identify the current activities of other industry groups that involve interoperability testing.

Recommendations

The IITC Oversight Group identifies the current activities of other industry associations relative to interoperability to maximize the efficiency of the interoperability testing effort.

6.5.5 Minimal Set of Scripts for Acceptance Testing

The previous sections have focused primarily on industry-wide interoperability tests. Another important phase of testing involves carrier to carrier testing that is to be conducted just prior to the interconnection of the two networks. This phase begins when a new local exchange carrier (*e.g.,* a CLEC) has turned up its network and is ready to interconnect to the network of the incumbent local exchange carrier. Tests need to be conducted to assure that each carrier's network is working properly. Currently, there is no industry-wide agreement on what tests need to be conducted to assure that each carrier's network is working properly. Consequently, a new carrier who opts to connect its network in several different locales to different incumbent local exchange carriers is faced with a wide variety of acceptance tests. A minimum set of test scripts for acceptance tests should be developed to be used nationwide to assure that each carrier's network is working properly before they are cutover for live traffic.

Once the networks are operational, new local exchange carriers can avail themselves of the incumbents test lines, *i.e.,* 105 test lines, to test/measure basic operational parameters. Guidelines for the use of such lines exist and are documented in the NIIF/NOF Reference Guide.

Recommendations

The NIIF under ATIS should be asked to develop a minimum set of scripts for acceptance testing to assure that interconnected networks are working properly before they are activated for live traffic.

6.6 SUMMARY

The Operations Task Group (OTG) of the Network Reliability and Interoperability Council Focus Group 1 has identified many of the most significant engineering and technical barriers to interconnectivity, interoperability, and accessibility to ILEC Operations Support Systems and Common Channel Signaling resources and associated operational issues with performance monitoring, security and interoperability testing. It has documented in this paper its key learnings and recommendations for the communications industry, the user community and the FCC to use to help mitigate those operational barriers. The OTG Core Team offers these recommendations in the true spirit of cooperation and optimism with the full knowledge that they describe a future end state at which the industry needs to be in order to fully support Section 256; not necessarily all the intermediate steps that will be implemented immediately.

A concise summary of the major recommendations are as follows:

- That Service Providers employ a robust, reliable, and secure electronic Gateway Interface for Operations System Access. The Gateway Interface will be built supporting TMN architecture, using pre-agreed "common language" for business purposes and data, providing for an automated Audit Trail, and be tested and benchmarked to establish minimum performance levels.
- That Industry continue to pay particular attention to the common channeling signaling networks upon which many new services are dependent, share relevant Industry information, be diligent about enhancing interoperability standards and testing, verify minimum performance levels for services, pay close attention to security issues, and implement an automated process to ensure ongoing signaling link diversity.
- That interconnecting parties specify in their Interconnection Agreements those parameters to be monitored to maintain normal business activities and pre-agree to the triggers and actions to be taken if those parameters go out of bounds.
- That Industry match the increased levels of interconnection and openness of the network with increased levels of awareness and implementation of available and soon to be available tools, techniques, strategies, and testing for security and reliability.
- That Industry continue to endorse and fund increased interoperability testing, with particular immediate attention being paid to stress testing of LNP, unbundling, and wireless/wireline integration.

6.7 SAMPLE DATA CONNECTION AGREEMENT

DATA CONNECTION AGREEMENT

This Data Connection Agreement dated as of _____ ("Effective Date") is between Belvedere ILEC, a Delaware corporation having an office at Belvedere Avenue, Belvedere USA("BELVEDERE"), and UTOPIA Corporation, a _____ corporation ("CLEC"), having an office at _____, _____ (UTOPIA)

WITNESSETH

BACKGROUND:

1. As stated in FCC Order 96-325, Paragraph 523, "We thus conclude that an incumbent LEC must provide nondiscriminatory access to their operations support systems functions for pre-ordering, ordering, provisioning, maintenance and repair, and billing available to the LEC itself. Such nondiscriminatory access necessarily includes access to the functionality of any internal gateway systems." Also from Paragraph 527, "Ideally, each incumbent LEC would provide access to support systems through a nationally standardized gateway." Elsewhere in this order, it is stated that if an incumbent LEC provides an electronic interface for its own users, it does not discharge its duties by offering competing providers access that involves human intervention, such as facsimile-based ordering.
2. BELVEDERE and UTOPIA are, or will be, parties to contracts under which one party (BELVEDERE) supplies telecommunications facilities, signaling, operations systems, operator services to the other, and agrees to provide unbundled testing and/or maintenance via remote access to the provided facilities and services (collectively, the "Network Interconnection Bilateral Agreement").
3. In connection with the Network Interconnection Bilateral Agreement, it is necessary or desirable to connect BELVEDERE ILEC data facilities with UTOPIA CLEC data facilities.

AGREEMENT:

In consideration of the foregoing premises and the mutual covenants and agreements set forth below, BELVEDERE and UTOPIA agree to connect BELVEDERE' data facilities with UTOPIA's data facilities as follows:

1. Facilities. The facilities to be used to connect BELVEDERE' data facilities with UTOPIA's data facilities are set forth on Attachment A. The parties will conform to the facilities specifications and requirements listed therein.

2. Term. This Data Connection Agreement is effective commencing as of the Effective Date, and will terminate upon the earlier of: (i) the termination of all the contracts

included in the Network Interconnection Bilateral Agreement, or (ii) December 31, 199X, unless the parties agree in writing to another termination date.

3. Information Transmitted ("Information").

(a) In General. The Information that is transmitted between BELVEDERE and UTOPIA pursuant to this Data Connection Agreement will be limited to such data as is necessary to carry out the intent of the Network Interconnection Bilateral Agreement.

(b) Information Transmitted or Accessed Under This Agreement Subject to Nondisclosure. BELVEDERE and UTOPIA will safeguard the Information transmitted between them under this Data Connection Agreement as confidential, highly sensitive data. Such information will be subject to all nondisclosure provisions of the Network Interconnection Bilateral Agreement. In addition, each party agrees: (1) to use the other party's Information only for the purposes specified in the Network Interconnection Bilateral Agreement, (2) not to reproduce the Information in any format, (3) not to reveal the Information to third parties except as required by law, (4) to take all reasonable precautions to safeguard the Information, and (5) to destroy or to return all of other party's Information (and copies thereof) to the transmitting party upon the earlier of: (i) the transmitting party's request during the term of this Data Connection Agreement or (ii) the termination of this Data Connection Agreement. This nondisclosure obligation shall survive the termination or expiration of this Data Connection Agreement.

4. Responsibilities of the Parties.

(a) Shared. (1) ACCESS FOR PHYSICAL SECURITY AUDIT: Each party will provide access to the other party during normal business hours, and upon a mutually agreed schedule, for the purpose of auditing the facilities used in the transmission or receipt of Information pursuant to the Network Interconnection Bilateral Agreement, to ensure compliance with the terms of this Data Connection Agreement. The right of audit includes, at a minimum, all of UTOPIA's systems or network endpoints that have access to BELVEDERE data. Visiting employees performing the security audit as described herein will be escorted at all times by an employee of the facility owner. (2) LOGICAL SECURITY AUDIT: Each party will permit the other, during normal business hours and upon a mutually agreed schedule, to perform logical security tests by technicians or automated equipment designed to identify potential security risks. These tests shall be limited to discovering risks associated with the usage and/or connections established pursuant to the Network Interconnection Bilateral Agreement.

(b) UTOPIA. The responsibilities of UTOPIA are set forth on Attachment B.

(c) BELVEDERE. The responsibilities of BELVEDERE are set forth on Attachment C.

Contacts. Operational contacts for Lucent Technologies and UTOPIA are identified in Attachment D.

5. Indemnification. Each party agrees to indemnify the other party and to hold the other party harmless for any loss or damages incurred as the result of: (a) the unauthorized access to the data facilities of the indemnified party through the indemnifying party's data facilities or equipment: (b) the misuse of Information obtained through the indemnifying party's data facilities, or otherwise obtained by the indemnifying party; or (c) any unauthorized access to, or misuse of, the data facilities, or Information of the indemnified party by the indemnifying party or any of its employees, agents, contractors, or other persons perpetrating such acts through the indemnifying party's data facilities or equipment.

6. Termination. Either party may immediately suspend or permanently withdraw access to its data facilities provided under this Data Connection Agreement, if (a) the other party fails to adhere to the provisions of this Data Connection Agreement, or (b) if the terminating party, in its sole judgment, believes there has been a breach of security or misuse of its Information.

7. Amendment. This Data Connection Agreement may only be amended in writing, signed by an authorized representative of each party hereto. This Data Connection Agreement supersedes and replaces all prior agreements, understanding, representations, promises and statements made by either party regarding the subject matter hereof. Attachments A through D are hereby incorporated by reference herein.

8. Assignment. The obligations and benefits of this Data Connection Agreement shall inure solely to the entities listed above, and not to any other entities, divisions or business units. This Data Connection Agreement shall immediately become void if it is assigned without the prior written consent of the other party, except that BELVEDERE may assign this Agreement to any successor entity or organization.

9. Execution. This Data Connection Agreement may be executed by the respective parties in counterparts, with each respective signature becoming effective upon receipt of a facsimile signature (original to be immediately delivered via overnight courier).

WHEREFORE, the parties authorized representatives have set their signatures below.

BELVEDERE		**UTOPIA**	
By:	**_____**	**By:**	**_____**
Name:	**_____**	**Name:**	**_____**
Title:	**Director of Corporate Computer and Network Security**	**Title:**	**_____**
Date:	**_____**	**Date:**	**_____**

ATTACHMENT A

[This section is an example of Facility Description]

FACILITIES DESCRIPTION

1. **Agreement to Private Line T1.5 Circuit in support of BELVEDERE StarWAN Services ("SWS") Partner Access, SWS3270.** Subject to the terms and conditions of this Data Connection Agreement, BELVEDERE agrees to permit UTOPIA to have access to the dedicated Private Line for the purpose of remote testing and maintenance of equipment in accordance with the terms and conditions of the Network Interconnection Bilateral Agreement.

2. **Private Line Specifications.** BELVEDERE will own, manage and provision one private line (the "Private Line") with the identification being: [circuit number, *i.e.*, DHEZ225310(T1.5)]. The Private Line shall connect the Tier III brouter [number, *i.e.*: C29ASP2 S0] located at the customer's premise at [address] to the Tier II brouter [number, *i.e.*: C29AST1 S6] located at [Data Center name, and address]. Two Data Set Units ("DSU's") will be provided by BELVEDERE to support the connectivity. The Internet Protocol addresses will be assigned by BELVEDERE System Engineers as follow:

Brouter/Port	IP Address	System
[To Be Completed]	[To Be Completed]	[To Be Completed]

3. **Backup Specifications.** BELVEDERE and UTOPIA agree that no backup circuit or dial access arrangement or any magnetic tape capabilities are necessary to fulfill the terms of the Network Interconnection Bilateral Agreement in any instance, including prolonged service outage or disaster of any cause, unless (and to the extent) such arrangements are specifically provided in any of the agreements included in the Network Interconnection Bilateral Agreement.

[This section is an example for CONNECT:DIRECT and interactive services]

ATTACHMENT B

UTOPIA RESPONSIBILITIES

1. USE THE "CONNECT Direct" product's features to provide for statistics and audit trails. The standard product offering support RACF exit points for each phase of execution before any data set allocation and after each functional request to interrogate the authority of the request or requests.

2. USE THE "CONNECT Direct" stage II security exit routine to base each user's authority on their read access to the ADMIN, OPER, and General User data sets. Once security is established for these data sets, any user wishing to access "CONNECT Direct" must have, at a minimum, read access to the General User data set to grant the ability to submit file transfer requests.

3. USE THE SECURED POINT OF ENTRY FEATURE TO DEFINE RACF Ids in BELVEDERE for non-BELVEDERE users, and place such IDs in the Authorization File, and correlate such IDs to the security ID of the external user. The specified ID will be verified with RACF and, if security validation passes, will be used for "CONNECT Direct" activities for that process.

4. THE COMMUNICATIONS INTERFACE FOR BELVEDERE, including Front End Processor, VTAM, SNI services, *etc.*, will be used to limit access by UTOPIA only to testing and maintenance of equipment supplied under the Network Interconnection Bilateral Agreement and to the resources specific to the contracted services.

5. All physical access to equipment and services required to transmit data in accordance with the terms of this Agreement will be in secured locations. Verification of authorization will be required for access to all such secured locations.

6. MODEM/DSU MAINTENANCE AND USE POLICY: UTOPIA will provide access to UTOPIA's facilities by BELVEDERE during normal business hours for maintenance of the DSU used for the transmission of Information as contemplated by this Data Connection Agreement. Use of any modem, DSU or Private Line for services not defined in this Agreement, including (among other things) dial up capabilities for modems, are forbidden. Any exceptions will require a written amendment to this Agreement.

7. UNAUTHORIZED USAGE DISCLOSURE: UTOPIA shall contact BELVEDERE Corporate Computer and Network Security within 24 hours of initial discovery of actual or suspected unauthorized access to UTOPIA's computing and/or network environment. Such a discovery jeopardizes BELVEDERE' data and network integrity connecting to BELVEDERE' data facilities or which could be connected to BELVEDERE' data facilities.

[This section is an example]

ATTACHMENT C

BELVEDERE RESPONSIBILITIES

1. BELVEDERE will be responsible for all networking components within the BELVEDERE [Data Center(s)] Data Center, including the Private Line circuits identified above, DSU's, front end processor (FEP), wiring and switches used to get to the FEP, router(s) and the mainframe connection.

2. All network-related problems will be managed to resolution by the respective organizations, BELVEDERE or UTOPIA, as appropriate to the ownership of the failed component. As necessary, BELVEDERE and UTOPIA will work together to resolve problems where the responsibility of either party is not easily identified. Notwithstanding this proposed procedure to resolve any operational difficulties which may arise during the term of this Data Connection Agreement, BELVEDERE reserves the right to disconnect the Private Line circuits at any time in accordance with Paragraph 6 of the main document.

3. All physical access to equipment and services required to transmit data in accordance with the terms of this Agreement will be in secured locations. Verification of authorization will be required for access to all such secured locations.

ATTACHMENT D

1. Regarding security problems, immediate contact will be made to the following security contacts:

For BELVEDERE INC:

Global Network Services Center:

1st Level Escalation: [Contact Name and telephone number]
2nd Level Escalation: [Contact Name and telephone number]
3rd Level Escalation: [Contact Name and telephone number]

Program Manager/Customer Interface:

(Name/Organization/Telephone Number)

For [UTOPIA]

1st Level Escalation: [Contact Name and telephone number]
2nd Level Escalation: [Contact Name and telephone number]
3rd Level Escalation: [Contact Name and telephone number]

Each party may change its contacts, as listed above, by giving written notice of the change(s) to the other party.

7. USER INTEROPERABILITY

Task Group 4, "User Interoperability" (originally named "CPE Group"), set out to determine whether there are any engineering or technical barriers or issues which might hinder the overall goals of the Telecommunications Act regarding interoperability and interconnection of telecommunications end users, and where such barriers exist to make recommendations to the industry for possible resolution, and if necessary recommend procedures for effective oversight of the resolutions.

Specifically, the task force looked to see if end users face technical/engineering barriers in connecting customer premise equipment (CPE) to networks and whether technical/engineering barriers exist in getting CPE to interoperate with other CPE designed for similar use. The term "end users" was interpreted by the group, considering language within the Telecommunications Act distinguishing telecommunications carriers from others, to cover those individuals, groups, and enterprises which have reason to connect their own equipment to a public telecommunications network, and who wish to interconnect and/or interoperate with other end users.

After exhaustive discussion and investigation into previous Network Reliability Council proceedings, issues, and recommendations, the User Interoperability task group determined that it would focus its efforts on whether the following conditions or issues create the end user barriers:

- increased interconnections
- high speed interfaces to end users
- interoperability testing
- network to CPE interconnection definitions
- adequacy of standards for vendor (CPE) compatibility
- impact on use of NRC II AIN and Best Practice recommendations
- connection of internet service providers to the public network

After some further discussion within the task group and with the NRIC Steering Committee, it was determined that the issue regarding "interconnection of Internet service providers to the public network" would be of sufficient interest in the foreseeable future that it would be appropriate to prepare a separate section on just this issue. While the same task group and team members did the work, the results of the work can now be found in Section 8 of this report.

In determining whether an issue identified by the task group needs action or oversight by the industry or the FCC, it is important to understand that there was consensus within the group that the end user market has been competitive for some time, and those competitive forces have generally been sufficient to resolve technical and engineering issues regarding CPE and interoperability. The issues considered by the group are based on the notion that the Telecommunications Act will in fact promote further beneficial competition within the industry.

This task force consisted of professionals from a wide spectrum of telecommunications companies. Members of the task group focused on specific issues, but all of the material was reviewed and discussed with all of the members, thus ensuring that the issues addressed were considered from an industry-wide perspective. In addition, all of the material proposed for consideration by this task group, including all versions of this report, the individual issues, the conclusions, and recommendations were posted in a timely fashion to the FCC's NRIC web site. To increase industry awareness of the task group's efforts, other industry groups (ATM Forum, Internet Access Coalition, ATIS IITC and several Committees of Committees T1, for example) were invited to comment. Finally, notices were also posted with two Internet news groups inviting comments and participation by all interested parties.

7.1 INCREASED INTERCONNECTIONS

The purpose of this section is to explore potential barriers or obstacles to reliability and interoperability as viewed by an end user as a result of an increasing number of interconnected telecommunications carriers, and to discuss whether adequate mechanisms are in place to address these concerns.

The user community welcomes the arrival of additional telecommunications carriers in the Public Switched Telecommunications Network. These additional players enhance the users' choices, stimulate industry innovation, and encourage the introduction of more cost effective services. The user community is keenly aware of these benefits. It is at the same time concerned with the potential impact on network reliability and interoperability as the number of interconnected telecommunications carriers that make up the national telecommunications network increases. This section explores the reliability and interoperability barriers associated with increased interconnection from a user's perspective, identifies how these barriers are being addressed, and discusses whether further action is required.

7.1.1 Key Learnings

Most of the barriers as observed from a user perspective are directly related to network-to-network interoperability and have been addressed by the Network Reliability Council Increased Interconnection Task Group II report (NRC II, "The Path Forward") or are being addressed by the NRIC Focus Group 1 and Focus Group 2 in other sections of this report. In addition, various bodies, groups, and industry associations (including the Alliance for Telecommunications Industry Solutions [ATIS] and the National Telecommunications Alliance [NTA]) have been formed to deal with these issues.

7.1.1.1 One of the largest barriers as viewed by users is the impact of increased interconnections on the standards development process, specifically on the timeliness and effectiveness of standards development in this new environment. The voluntary telecommunications standards process is the primary tool for defining the interfaces that make user equipment interoperable.

As marketing/technology developments materialize at an accelerated rate as a result of the increased competition in the telecommunications and computing industries, it is even more imperative that the standards process keep pace with these developments. Users forced by their market demands to implement a technology prior to the completion of standards are faced with the difficult and confusing task of deciding which of the various competing products/solutions to implement. Often, users are saddled with absorbing the cost of obsolescent pre-standard (*i.e.*, proprietary) CPE investments.

In fact, users fear that while standards development needs to be accelerated to improve timeliness in responding to market needs, the introduction of a greater number of interested parties and stakeholders might actually result in even slower standards development. The increased number and types of telecommunications carriers (with diverse views and divergent desires based on the strengths and limitations of their respective networks) may exacerbate standards development problems.

In addition to impacting the timeliness of the standards development process, the presence of additional players could also adversely impact the effectiveness of new standards work, compromising the quality of new standards work. For instance, a new standard might not be as sharply defined as possible to accommodate the interests of the various players, or a new standard might provide alternatives in order to appease the various parties. A standard that is not well-defined will be subjected to different interpretations by service providers, resulting in end-to-end incompatibility. A standard that allows for alternative implementations still burdens the user with deciding which of the competing technologies to implement, or may result in more costly CPE devices designed to work with the various options.

In some situations, communications takes place between "major" telecommunications carriers and CPE manufacturers to implement procedures to resolve CPE-Network-CPE interworking issues. The interaction between the Vendor's ISDN Association and the National ISDN Council is one such example. In some cases, it proves to be difficult to transfer these new procedures on the user interface to other service providers.

One final concern of users regarding standards development is the increased difficulty for the user to influence or provide input to standard development due to the increased number of players and the decentralization of this process.

7.1.1.2 A second barrier associated with the introduction of increased interconnections is user uncertainty regarding continued functionality and reliability of existing services when interconnected with new networks. First, users could experience difficulty determining whether existing vertical services continue to work when a new service provider is used to carry part of the call. For instance, will a customer lose some or all CLASS functionality when part of the call is handled by another service provider? Second, when two different network types are interconnected (*e.g.,* wireline and Cable TV) or when one network type is used for multiple applications (*e.g.,* telephony and video), how is the combined reliability and survivability determined? The user needs to be educated or informed whether the requirements currently in

place for wireline subscribers such as availability of dial tone and access to public safety will be applicable to other telecommunications carriers or in an interconnected environment.

7.1.1.3 A third barrier is user concern regarding fault isolation and service restoration. In situations where a user whose service consists of various service provider components in an interconnection arrangement experiences trouble, the user is burdened with determining where the fault resides in order to report the trouble to the proper service provider. The user's ultimate fear is the scenario where the user continues to experience a trouble, yet all of the various telecommunications carriers report that their respective components are in service.

Fault isolation and service restoration issues have existed for data services for many years, and are well understood. Data users have learned to perform end-to-end troubleshooting of a circuit that consists of several interconnected components. As a result, this barrier is more of a concern to users of voice services since they are not as familiar with the issues and have no prior experience in this area.

7.1.1.4 A fourth obstacle associated with increased interconnections as viewed from a user perspective is the potential to experience increased response times (post dial delay, *etc.*) or possibly suspension of calls (if call handling data cannot be successfully passed) due to screening and mediation activities occurring between interconnected networks. As more and more networks are interconnected, there are more opportunities for calls to be "handed off" from one network to another. As experienced following divestiture, there may be end user frustration with increased delays for connections to be made and verified.

The concern of increased response times is not new, and the FCC has provided oversight in the past for undertakings such as SS7, Equal Access, and Local Number Portability.

7.1.1.5 A fifth issue is billing integrity. End users might have concerns regarding billing accuracy in an interconnected environment. This concern stems from the current difficulty for telecommunications carriers to verify the integrity of billing data being passed between them. It seems obvious that with more interconnected networks, billing data may become more difficult to verify, and where the end user feels that billing is in fact incorrect, it may become more and more difficult to have correcting adjustments made.

7.1.1.6 A final barrier is related to users who wish to gain access to Intelligent Network (IN) components of the national telecommunications network. Large end users (*e.g.,* private network providers) desiring IN connectivity may experience difficulty in confirming the successful passing of call handling data.

For instance, an end user who operates a large private network might wish to utilize IN capabilities in order to interconnect with the pubic network and process calls more efficiently, or access IN features such as time-of-day routing. An end user could also create and define a service that is needed temporarily via his own Service Creation Environment (SCE) terminal.

7.1.2 Recommendations

7.1.2.1 The industry should closely monitor the proliferation of industry associations and fora involved with access standards development to guard against the negative effects associated with the decentralization of standards development. It is important to acknowledge that these groups have had an extremely positive effect on standards development, to date. If the industry determines in the future that the quality or effectiveness of standards is being compromised, or the timeliness of the standards development process is being adversely affected, then the industry should consider forming a special end-user focused task group to address this matter.

The NRIC Focus Group 2 addresses standards issues more comprehensively in Section 9 of this document. Section 9.4.3 includes specific recommendations to the FCC including the establishment of a single point of contact to facilitate the exchange of information between the FCC and standards developers; ongoing monitoring of standards activities; and oversight in addressing standards related complaints.

Further discussion:
Industry fora that include users as integral members and contributors (such as ATM Forum, North American ISDN Users' Forum, and the Intelligent Network Forum) should be encouraged to allow users the opportunity to actively participate and influence standards development. The standards definition procedure should be made available to all stakeholders in the industry in order to hear all points of view. It is also important to recognize that industry fora can have a detrimental effect on the standards development process if stakeholders engage in "forum shopping" to participate in fora or establish new fora that support their needs. To date, the benefits of these industry fora to users have outweighed the negative effects on the overall process.

The ANSI accredited democratic process currently in place with several groups and industry associations working closely should be maintained, as well. The Alliance for Telecommunications Industry Solutions (ATIS) sponsors various committees deeply involved in standards work, such as the Network Interconnection/Interoperability Forum (NIIF), and Committee T1.

Users are also uncertain regarding Bellcore's future role in the management of generic requirements due to a change in ownership currently underway. Under the ownership and direction of the RBOCs, Bellcore has played a significant role in developing generic requirements such as generic requirements for network services, equipment, and network interconnection signaling. This Task Group believes that competitive forces will drive Bellcore or other industry fora to develop generic requirements. It is critical that whatever group develops such requirements, the process be open and reasonably available for participation by all interested parties.

As suggested in the NRC II report, to expedite the standards development process, interactive electronic access methods should be employed and a schedule with milestones and deliverables employed. The NRIC Focus Group 2 addresses standards development process issues in greater detail in Section 9 of this report.

Developing an effective standard requires striking a delicate balance. As suggested in the NRC II report, to improve compatibility, standards should have a sharp technical focus and standards bodies should strive to minimize the complexity and optionality of requirements. At the same time, standards should focus on achieving a basic level of interoperability, and should not be so specific as to stifle innovative approaches to a problem. The development of baseline standards will ensure that network elements can accomplish their basic function without impairing the network, and that user-to-user functionality will be achieved. Section 7.5 of this report titled, "The Definition of 'Adequate' Standards for Vendor Compatibility" discusses user interface standards.

It would also be beneficial to create a facility for various groups to test interoperability in a captive network, and in a low profile environment that allows engineers to communicate to resolve interoperability issues. This is discussed further in Section 7.3.

7.1.2.2 The Council recommends that the FCC develop a short list of nationally accepted services and require that no telecommunications service provider make any system-wide changes in or extensions to such services that would cause a subscriber to lose such services unless those changes or extensions (1) are the product of the National Planning Process discussed in Section 4 above and (2) provide an opportunity to the customer to maintain uninterrupted service.

Further discussion:
The legislative concern for continued functionality by end users is evident in Section 256 of the Telecommunications Act of 1996, which states that "seamless interoperability" is expected in an interconnected environment. While maintaining functionality when a user changes carriers, CPE, or services is paramount, the strictest interpretation of "seamless interoperability" would be impossible to achieve and would stifle innovation and competition. As a result, "seamless interoperability" would be applied rigorously to the short list of national services.

Developing and existing industry organizations are concerned with promoting reliability and interoperability. For example, the National Telecommunications Alliance (NTA) was recently formed to assume Bellcore's historic role of enhancing the interconnection, interoperability, reliability, and security of the national telecommunications network. The RBOCs formed the NTA to fulfill their common goals of safeguarding the national network, and serving as single point of contact with the Federal Government for National Security Emergency Preparedness (NSEP).

Resolution of potential functionality issues is handled by the ATIS sponsored NIIF and Internetwork Interoperability Test Coordination (IITC) Committee. Reliability issues are handled by the ATIS sponsored Network Reliability Steering Committee (NRSC).

The existing telephone network was built to conform to stated specifications, (*e.g.,* LATA Switching System Generic Requirements [LSSGR] developed by the Regional Bell Operating Companies, through Bellcore). Consideration must be given to whether a minimum set of

requirements is needed to protect reliability in the interest of the end user. If a minimum set of requirements is not established, the end user could decide which service provider to use by comparing functionality, reliability and cost, but the goals of maximum access and seamless interoperability could be lost. Survivability and reliability from a user's perspective are addressed further in the Network-to-CPE Interconnection Definition section (Section 7.4) of this document.

7.1.2.3 Performance monitoring and testing efforts within the industry, already acknowledged and accepted by the FCC, should continue under ATIS and are discussed further in Section 7.3 of this report. No additional oversight is required.

Further discussion:
Fault isolation and service restoration are directly related to network-to-network reliability and are also being addressed by the NRSC under ATIS. The NRIC Focus Group 1 Operations Task Group discusses this matter in greater detail in Section 6 of this report.

Another solution is to become more proactive in trouble isolation by involving CPE (*e.g.,* terminal equipment, private network equipment, *etc.*) vendors up front to participate in standards development for the introduction of new services. CPE vendors can build testing and monitoring capabilities into devices that can provide messages in the event of a network failure. These messages can be used by the user and service provider to help isolate a trouble. The current industry has already begun to address trouble isolation. While network-to-user interfaces have become more sophisticated, network intelligence has moved closer to the user in the form of more sophisticated CPE. For instance, the Vendor ISDN Association (VIA) has been working with the National ISDN Council (NIC) on building diagnostic capabilities into ISDN devices.

7.1.2.4 No additional action is required to address increased response time and call suspension issues associated with increased interconnections. NRC II recommendations are adequate.

Further discussion:
Delayed response times and suspension of calls are real user concerns. These matters are adequately covered under the previously mentioned network-to-network task group efforts. For example, the NRC II report recommends that industry associations such as ATIS (IILC Issues 052 and 053) and TIA consider the value of incorporating performance requirements with the interface standards requirements. Network-to-network implementation issues are covered further in Section 5.

7.1.2.5 Billing issues are being addressed under ATIS. No further action is required.

Further discussion:
Billing accuracy is directly linked to network-to-network issues being addressed by the NRIC Focus Group 1 Operations Task Group (see Section 6) and other industry associations, such as the ATIS sponsored NIIF, Ordering and Billing Forum (OBF), and Telecommunications Industry Forum (TCIF). Some solutions being considered include mechanized billing and third party access to billing (which introduces security and system capacity concerns).

A more simplified, total billing data collection system with standard data passing formats and media would greatly improve billing accuracy and timeliness for the end user.

7.1.2.6 If third party access to Intelligent Network components is extended to include the user community, the industry should develop a template (see Section 7.5) to allow for the successful passing of call handling data. This template can be based on the Network-to-Network template, as discussed in Section 5.2.

Further discussion:
Currently, third party access to Intelligent Network elements is limited to telecommunications carriers eligible to make interconnection/unbundling requests under Section 251 of the Telecommunications Act of 1996. Furthermore, it has been industry/best practice to limit access to Intelligent Network elements in order to safeguard this critical piece of the telecommunications network.

The need to safeguard the network must be carefully weighed against the desire of end users to access Intelligent Network capabilities. Given the difficulties and uncertainties that have already been identified surrounding third party access to carriers, plus the major concerns relative to network reliability and competitive information, the industry should first proceed to resolve current issues associated with third party access for carriers, and then use those lessons to carefully open access further. End users, aware of the damage that viruses have caused in the PC/Internet environment, can understand the destruction that can be inflicted on the telecommunications network.

The Intelligent Network Forum, an industry association comprised of vendors, users and carriers, and the NIIF (see IILC Issues 026, 049, 050, and 057) are looking at the issues associated with providing third party access for end users, including end user needs for this capability, technical feasibility, contention issues, and risk of causing significant network outages. Section 7.6 discusses the applicability/extension of user interfaces on AIN.

7.2 HIGH SPEED TO USERS

7.2.1 Scope and Background

The purpose of this section is to consider technologies offered to users by carriers that offer transmission rates of higher than T1 (1.544 Mbit/s). Opportunity to comment was offered to the general community via postings to the comp.dcom.cell-relay and comp.dcom.telecom news groups of the Internet.

The technology choices for offering high speed service to users are numerous and increasing, but still not widely deployed. Many different services are provided that go far beyond simple interconnection for the transmission of undifferentiated bandwidth. There are a very large

number of standards and technologies involved in, for example, the provision of Internet web-site hosting and access over xDSL over the existing copper loop to the home. A mismatch in any one of these between the user equipment and the network equipment can make communication impossible. Yet the competitive nature of the marketplace means the change in all areas of the technologies is far outstripping the development of standards, and indeed is promoting an ever-increasing diversity of options.

Implementation of all of the options is impossible for both carriers and users, and the marketplace plays an effective role in limiting the diversity while at the same time promoting innovation and interoperability. It should be noted that not all technologies will be available to everyone since field deployments can be regional in nature. (See Section 4.)

Users of the new high speed services are typically companies or government, rather than individuals. Their choice to use a new technology is based on the benefits that the new technology offers, and they weigh that against the possible impacts of adopting that technology for part of their telecommunications needs. It is quite likely today that the users would choose to maintain traditional voice telecommunications services as well, depending upon them for the seamless interoperability they bring.

For these reasons, it is premature to suggest additional levels of oversight for these new high speed services until and unless specific issues arise once the services have gained sufficient importance in the marketplace to be considered a national service.

None of the high speed technologies are mature enough to be current candidates for the national list. They do, however, have the possibility of becoming a part of this list as the technologies mature in the marketplace, and become less proprietary in nature, allowing a more ubiquitous interoperable deployment.

7.2.2 Key Learnings

7.2.2.1 Asynchronous Transfer Mode (ATM)

Most deployment of ATM today is to handle user data. There are products available for carrying voice over ATM, and at least one carrier is offering this as a service. On the standards front, ATM is being studied in recognized standards bodies (*i.e.,* ITU-T) as well as in organizations which are not formally so recognized (*e.g.,* the ATM Forum). Still other products being sold offering capabilities not yet submitted for standardization. As is common in many areas, these groups co-operate, but this does not necessarily result in agreement. Particularly in the ATM Forum, the desire to minimize costs within private corporate networks typically overrides concerns expressed by public carriers for network stability and diagnosability. A particular example is the definition of ATM interfaces not capable of carrying network synchronization information.

The issues revolving around ATM encompass standardization and interoperability, cost, and reliability.

7.2.2.1.1 Standardization and Interoperability

ATM standards are still in the evolutionary stages with additional vendor implementations that are proprietary in nature. The network and CPE based connectivity and reliability issues associated with ATM are currently being addressed by the ITU standards group and the ATM Forum. Services over ATM are being addressed in several additional fora, including the IETF, DAVIC, Winsock, and the APPN Implementors Workshop. Most of these other groups have liaisons with the ATM Forum or the ITU, and the ITU and ATM Forum have liaisons with each other.

The rapid introduction of different alternatives to carry voice over ATM in different formats will make it challenging to ensure compatibility between different users' equipment and different carriers' services, as well as embedded public switched telephone networks. Because of the many variants of voice over ATM, users will have to work directly with their voice service provider if they wish to interwork the user's technique for handling voice over ATM with the carrier's voice service. This is true also for interworking voice services between embedded public networks and ATM carrier networks. Therefore, ubiquitous deployment of ATM may be hindered due to interoperability issues between manufacturer’s products and telecommunications carrier’s implementations. Electrical and optical network interface connectivity issues and standards will need to be finalized prior to vendor compliance.

7.2.2.1.2 Cost

ATM can typically be implemented at a lower bandwidth via existing copper facilities using T1 services and/or ADSL technologies. Since fiber cable may not be deployed to most customer premises and ATM electronics are high priced, it may not be cost effective to construct the service. Bandwidth demand may not be enough to drive deployment at this time.

7.2.2.1.3 Reliability

Reliability is based on vendor specifications and may vary from one manufacturer to another. Redundancy may be derived from electronics or from network infrastructure. If a public carrier must provide an interface to an end user with sufficient isolation, redundancy, and reliability to prevent impacts on the public network, the public carrier may:

- have to expend sufficient additional cost compared to value-added network operators not so constrained so as to be not competitive, and/or
- be forced to not support features available with private signaling because of lack of adequate signaling robustness and scalability, again putting the public carrier at a competitive disadvantage.

Both of these possibilities can impact availability, accessibility, and interoperability as seen from the point of view of an end user.

7.2.2.2 Asymmetrical Digital Subscriber Line (ADSL)

There are several issues regarding network reliability with ADSL access technology.

7.2.2.2.1 Standards

Standards have been set by the ANSI T1E1 subcommittee; however, they are not universally available at this time and are different from the solutions that are currently in the marketplace. Discrete Multitone (DMT) was determined to be the line code of choice. This coding scheme was preceded by Carrierless AM/PM (CAP) which entered the marketplace approximately one year prior to DMT and has been deployed in multiple field trials throughout the country. This also raises the question of interoperability between manufacturers. Even though a vendor may use a standard line code, the vendor may also incorporate a proprietary protocol. This can cause interoperability issues for end users.

For example, if users buy an ADSL modem in one territory and chooses to relocate, the new location offering may include a different ADSL vendor. This will render the customers' current modems useless for this application and would require them to purchase new devices to enable service.

In addition, the format of the content within the line coding is also still under debate. If the format is ATM, all of the issues above are relevant. If some other format is used, the same issues being addressed by the standardization and implementation efforts for ATM will be faced for that format as well.

7.2.2.2.2 Local Loop

Although ADSL provides an end user a high speed technology for use over local loop copper facilities, it is not a ubiquitous technology. ADSL will not function on all local loops, therefore is not likely to be implemented in every location. It is estimated that ADSL will operate on only 50-80% of the loop facilities in today's network. ADSL has a distance and bandwidth limitation based on the electrical characteristics of the copper cable it is transmitted over. Since the outside plant engineering design philosophies may differ between telecommunications providers, the performance of ADSL will differ also.

7.2.2.2.3 Spectrum Compatibility

There are interference issues involved when mixing the ADSL technologies (DMT and CAP) with traditional lease lined services (T1, ISDN, 56Kbps). ADSL technologies cannot reside within the same cable binder groups as the legacy digital services and sometimes may cause problems in adjacent binders. These may manifest themselves in many ways including lower bandwidths, distance limitations and often total inoperability. Spectrum compatibility needs to be addressed to resolve these potential interoperability issues.

7.2.2.2.4 Customer Premises Wiring

There are several alternatives to location of the POTS splitter(s) in the ADSL network scenario, and as usual there are advantages and disadvantages to each.

- Network Interface Device (NID): When locating the splitter at the NID, POTS transients may get into the ATU-R by crosstalk
- Asymmetrical Termination Unit-Remote (ATU-R): When locating the splitter at the ATU-R, POTS transients can get into ATU-R by crosstalk and in-house bridge taps which may be in the ADSL path
- At every phone: If the splitters are located at every phone receptacle, the expense of multiple filters, in-house bridge taps, and degradation of ADSL margin may become an issue.

7.2.2.3 Cable Modem Technologies

Cable modem technologies do not follow any set standards, therefore all vendors have a proprietary product today. It should be noted that a group of manufacturers recently announced an intent to build interoperable devices. Not only is the network side of the modem currently proprietary, the CPE interface may be also. If a customer purchased a cable modem and chose to relocate, this modem may not function at their new home depending on the vendor implementation. Much like the ADSL example, the customer's modem would need to be replaced with that of the appropriate vendor to enable service.

There are open technical issues with regards to noise on the upstream path inherent to this technology. With their embedded networks and existing technology, it is estimated that 90% of the cable TV operators do not have a return path to accommodate any upstream bandwidth. Conversely, most local telephone companies do not have cable deployed.

7.2.2.4 Integrated Services Digital Network (ISDN)

The major issue with ISDN is the lack of deployment within the independent telephone company industry. This technology is not ubiquitous at this time although there are indications that this technology is being adopted by end users at a fast pace.

7.2.2.5 Local Area Network (LAN) extension

Several carriers are offering services extending ethernet, token ring, and /or Fiber Distributed Data Interface (FDDI) across the network. Carriers are offering such LAN-based services utilizing multiple technologies, and defining multiple services. This supports the call for innovation. Some of the services include CPE or service provider equipment located at the end user’s premise, while others don't. Some are point to point, while others are multipoint to multipoint. Some are transparent to user address plans (*i.e.,* bridged), while others are not (*e.g.,* routed). Given that the standards for ethernet, *etc.*, are well established in the industry, with an established standardization process in IEEE, there are no known issues regarding network reliability or interoperability.

It is possible to make cheaper equipment or system selections that do not have sufficient reliability, but it is also possible to provide a costlier reliable service using network and equipment redundancy.

7.2.3 Recommendations

7.2.3.1 The task group believes that the marketplace will best resolve end user interoperability issues. The existing market interactions and standards process should proceed until these technologies are widely enough deployed to make it possible to determine what issues become important. If these are not already under study in the various standards and industry bodies when that occurs, they should be referred at that time by industry contribution. The government should legislate a solution only where it appears voluntary action is not meeting a compelling national need for interoperability (see. *e.g.,* Sections 4, 6.2.3 *etc*.).

7.2.3.2 To guard against undesired interference, the FCC should continue oversight under Part 68 of new technologies applied to unbundled loops.

Further discussion:
When a single telecommunications carrier is responsible for deployment of new technologies in the existing access plant, it can by itself ensure that technologies deployed in adjacent cable wiring do not interfere with each other. With loop unbundling comes the possibility for more than one carrier to deploy more than one new technology in an uncoordinated manner, such that while neither interferes with legacy voice applications, they interfere with each other.

7.3 CPE INTEROPERABILITY TESTING

7.3.1 Introduction

Section 3 (14) of the Telecommunications Act of 1996 defines "customer premises equipment" (CPE) as "equipment employed on the premises of a person (other than a carrier) to originate, route or terminate telecommunications." The purpose of this section is to consider the role of testing in ensuring the proper functioning of CPE with the diversity of networks designed to accommodate it.

One consequence of the Act is the likely emergence of numerous special purpose networks. These networks will need to interoperate with each other for the completion of the telecommunications function. And access to this 'network of networks' will need to be ensured if end user's CPE will also interoperate to satisfy the telecommunications objective.

The work of the Task Group began with the identification of several key issues related to the question of CPE-network interoperability testing compiled from the responses of the NRIC

membership survey conducted by Focus Group 1 Chairman, John Gunter. The replies suggested that:

- The existence of standards is necessary but not sufficient to ensure interoperability,

- Section 256 of the Telecommunications Act of 1996 requires CPE to interoperate in order to be connected to the network, and

- Innovation will be inhibited without the flexibility to extend standards at least to some degree creating some level of nonconformance to standards and non interoperability.

The Subcommittee investigated the activities of existing industry standards bodies, the decisions of the FCC to date, and the interests of independent testing laboratories in the private sector. The Subcommittee also considered the duty of the FCC to promote innovation within the network as it studied the issue of ensuring CPE interoperability

7.3.2 Key Learnings

Key learnings have emerged from each of the areas of study relating to the standards bodies, actions of the FCC, and activities within the industry.

7.3.2.1 Existing Standards Bodies

Section 9 includes a comprehensive review of standards bodies in telecommunications. The purpose of this discussion is to focus on those addressing CPE issues.

Section 256 (b) of the Telecom Act assumes the existence of standards bodies for the purpose of defining interoperable CPE. Such organizations relating to CPE were, in fact, found to be well established. (See Section 9).

Despite the existence of standards bodies supported by industry consortia, there are still two areas of deficiency related to ensuring interoperability of CPE. First, standards documents can never be wholly unambiguous in their interpretation. The International Telecommunication Union (ITU) is working towards the goal of making standards less ambiguous, but much work remains to be done.

A Swedish software design firm, Telelogic (www.telelogic.com) has developed an object oriented SDL based language for the writing of standards that are both testable and implementable. The ITU is testing this tool with the goal of producing standards that can be tested for conformance during the development cycle of the product itself.

The second deficiency in the area of CPE standards is the fact that no standards body accepts the responsibility of testing for compliance to the standards which they create. While vendor participation in standards processes can reduce ambiguity, vendors otherwise are on their own when interpreting standards while developing their products. Buyer's must realize that the

equipment they purchase may not fully interoperate with similar equipment produced by another vendor. Compliance tests are necessarily selective, and narrowly prescribed to the specific commercial applications of the product at that moment.

7.3.2.2 FCC Actions

In 1992 the FCC's first Network Reliability Council (NRC I) endorsed the Internetwork Interoperability Test Plan (IITP) chartered by the Network Operations Forum. Over twenty LEC and IXC vendors came together to test SS7 interoperability under stress conditions. Bellcore acted as facilitator of this process with the each participant paying its own expenses. Over 200 anomalies were found that contributed to a reduction in the outage index.

In 1994 NRC II endorsed the recommendations of its Network Interconnection Task Group. The Group proposed to expand the current processes to include future interoperability tests in a nationally coordinated program under the management of the Alliance for Telecommunications Industry Solutions (www.atis.com). Thus, in 1996 the Internetwork Interoperability Test Committee (IITC) was organized, although specific proposals for how the industry will maintain the IITC beyond mid year 1997 have not been settled.

Interviews with the membership of the IITC have found them interested in further expanding the scope of its IITP to include CPE to network interoperability testing.

Examination of the current FCC Part 68 certification procedure found it to depend on the work of private-sector test laboratories to provide assurance that CPE satisfy the required physical and electrical specifications. The FCC too, has stated its willingness to amend its Part 68 specifications to accommodate new technology or testing criteria to ensure interoperability. Part 68 currently is principally concerned with specifications to ensure protection from network harm.

7.3.2.3 Industry Actions

Investigation has revealed that many organizations besides ATIS are interested in interoperability testing. Programs for interoperability testing can be found in both the telecommunications and computer industries. The CTIA has an excellent model program, and PacBell (www.pacbell.com) works collaboratively with the California ISDN Users Group (www.ciug.org) in the sponsorship of an annual ISDN CPE interoperability certification.

The Cellular Telecommunications Industry Association (www.ctia.org) has established a Certification Program that evaluates the performance of cellular subscriber equipment. The program incorporates extensive testing based on industry standards from EIA/TIA. The CTIA interoperability testing program includes 61 parameters whereas the FCC Part 68 requirements contain only five, and the Canadian CRC consists of but thirteen parameters.

The CTIA program is strictly voluntary and was created at the request of the carriers. The CTIA contracts the testing to independent testing facilities, while retaining control of administrative procedures and the test requirements document.

When a cellular phone passes certification the manufacturer earns the right to exhibit the CTIA certification seal on the phone and its packaging and to use the seal in its advertising. This seal, which signifies to consumers that it meets or exceeds all technical standards, is good for eighteen months, after which the phone must be retested or must stop using the seal. The CTIA reserves the right to require retesting of certified units at any time to assure compliance.

The computer industry is replete with examples of voluntary interoperability testing. One notable example is the Network Interoperability Alliance (NIA) formed in May, 1996 by the seven major computer networking companies. A multivendor networking environment has been created in the University of New Hampshire Interoperability Laboratory (www.iol,unh.edu/consortiums/indes.html) dedicated to conformance testing of network products in actual customer environments. Going beyond typical multivendor tests that use basic tools such as 'ping' to test for connectivity, the IOL uses actual applications traffic, including web-browser to server and network file sharing to facilitate its testing. A second round of tests is planned to test system level network management (RMON) and Token Ring over ATM.

Private-sector, independent laboratories are also cautiously interested in performing interpretability tests for public network CPE. Select laboratories that offer such services in the computer networking area include the National Software Testing Laboratory (www.nstl.com), Veritest (www.veritest.com), and XXCAL (www.xxcal.com) and many others. Bellcore (www.bellcore.com) is expected to become an independent laboratory soon, and also offers some interoperability testing services.

Novell and Microsoft have certification programs typical of those found in the computer industry that uses these testing laboratories. Only servers that are 100% compatible with Novell software are permitted to display the Novell YES program seal. The Microsoft WHQL seal has a similar meaning relative to its software.

Independent certification testing laboratories conduct the tests necessary to determining that a server passes the interoperability tests required to merit the software vendor's seal of approval. Government contractors are required to have this seal in order to be selected as a vendor.

When queried about the prospects of a CPE interoperability certification program these test laboratories were only cautiously interested in CPE because of their concerns about whether they could write the necessary tests and specifications, invest in the necessary test equipment, and secure the necessary new skills.

7.3.2.4 CPE Is an Important Source of Network Innovation

The subcommittee recognizes the CPE interoperability standards and guidelines are essential for proper network operation. Section 256 of the Telecommunications Act of 1996 is designed to address this requirement as it directs the FCC to "promote nondiscriminatory accessibility by the broadest number of users and vendors… to ensure the ability of users and information providers to seamlessly and transparently transmit and receive information." Yet other Federal statutes

relating to lifeline service can not be satisfied without well defined standards for this basic interoperability.

At the same time, Congress has mandated that the FCC seek to promote technical innovation within the network. To that end, note must be taken of the special contribution user innovation has made to network evolution. Numerous examples can be found of new functionality in private networks that has migrated into the public network, including custom calling services, voice mail, ACD, *etc.*

Since this historical trend is likely to continue, any interpretation of CPE interoperability must be tempered by the objective of preserving this source of network innovation. Extensions to the basic interoperability standards essential to public safety must continue to be tolerated as they have been in the past so as to permit experimentation by individual users, so long as they do not interfere with the communications ability of other users.

Innovation, deregulation, and competition are at odds with the concept of "seamless interoperability." Standards to insure proper operation must be rigidly enforced between networks, and between the network and CPE to preserve basic lifeline services. But various extensions to these network-CPE standards to promote innovation are viewed as desirable.

7.3.3 Recommendations

Focus Group 1 proposes three recommendations as follows:

7.3.3.1 The telecommunications industry should maintain the voluntary standards process.

The private sector has created an extensive framework of standards-setting activity based on voluntary collaboration. The FCC need not assert its regulatory influence in this process other than to assure that standards continue to be set quickly and be created in a way that helps stimulate competition and innovation. Section 9 of this report, representing the work of Focus Group 2, addresses standards issues in great detail.

7.3.3.2 The telecommunications industry must take action to ensure CPE interoperability

As no standards body enforces its standards other means of assuring compliance is required. The dictates of the dominant local exchange carrier had been the primary mechanism through which this goal was achieved in the past but cannot be relied on to play this role in a competitive environment.

In the network of networks a new mechanism must be found. The free market is a potential, but inefficient ad hoc processes could jeopardize public safety if used as the sole mechanism for assuring CPE interoperability.

To that end the NRIC encourages the industry to create a CPE interoperability program for the FCC's list of national services as outlined in other sections of this report.

One way to do this would be to request that ATIS extend the charter of the IITC beyond network to network interoperability testing, and include network to CPE interoperability testing for the list of essential FCC services. ATIS could possibly model a public network certification program after that being used in the cellular sector or the computer networking industry.

The industry could ask ATIS to establish a certification seal for the essential services required for public safety along with the interoperability criteria. Private sector test laboratories could then conduct certification tests as a necessary criterion for FCC Part 68 registration. In addition, there should be a program of manufacturer self-declaration to the interoperability criteria.

7.3.3.3 Standards extensions must be tolerated to stimulate innovation.

In prescribing a means of ensuring CPE interoperability for public safety in the network of networks, it is equally important to protect the source of innovation represented by CPE and its interaction with the network.

To that end the FCC should explicitly express its position regarding extensions to the standards for CPE interconnection to the network. Criteria for such tolerance should include preservation of basic interoperability for public safety, competitive fairness, and any other matters of public interest.

7.4 NETWORK-TO-CPE INTERCONNECTION DEFINITION

7.4.1 Key Learnings

The need for a Network-to-CPE Interconnection Definition was identified by the Focus Group 1 User Interoperability Task Group as one of the key issues in reducing interoperability barriers.

The concern raised is that there is no standardized document which provides sufficient technical guidelines about interconnection requirements between a common carrier network and user CPE. Lack of such a guidelines document, including adequate supporting industry standards, has created situations where CPE has been built that functions as expected when connected to one public network, but does not when removed and connected to a different network. As discussed in the Section 7 introduction, it is not realistic to expect "seamless" interoperability of CPE in all networks given the highly competitive and rapidly changing telecommunications environment. End users do expect, however, their CPE to be "portable" for a baseline set of services that are offered ubiquitously (*e.g.,* the standard push button telephone set and its support of multiple calling features).

Traditionally, common carrier network providers have issued Network Disclosure statements as a means of outlining their interconnection requirements to interested CPE and network equipment manufacturers, but the constant introduction of new technologies, features, protocols, *etc.*, has

made it necessary that more detailed, specific information be made available than is normally provided. When new services are introduced, such as Wireless services, Hybrid Fiber Coaxial services, Internet services, *etc.*, supporting standards often lag behind. This increases the potential that interconnections will fall short of the user's performance expectations because of unresolved technical issues. (Note: This is clearly the case in the "Network-to-Network" interconnection arena, where the promise of industry standards defining full interoperability between any two vendor's SONET network elements is yet to be realized). An interconnection that is not fully defined by the network provider may lead to problems due to service disruption or additional costs forced on the user to replace or modify installed CPE.

7.4.2 Recommendations

A crucial step in eliminating barriers to interoperability is to establish a document expanding on current Network Disclosure statements that clearly and precisely defines the technical criteria and standards to be met by CPE and network equipment manufacturers when building a device for a particular type of Network-to-CPE interconnection. A document in the form of a specifications template has been developed that serves as a guideline for Network-to-CPE interconnection. This template categorizes and briefly describes technical specifications that may be useful in building a Network-to-CPE interconnection.

It is required that network providers disclose Network-to-CPE interconnection specifications to interested network and CPE manufacturers so that they may design equipment to meet Network-to-CPE interconnection requirements, or so that users may purchase compatible off-the-shelf CPE. The proposed template is intended to help network providers furnish detailed, relevant information that covers the majority of Network-to-CPE interconnection issues that should arise, but it is only offered as a guidelines document. It is a checklist of technical areas-of-concern to be considered when describing a specific Network-to-CPE interconnection scenario.

It is important to note that certain interconnection arrangements will not fit the template entirely and may require that some different parameters be specified than those identified. In any case, a sufficient amount of detail is required to ensure that equipment designed to the specifications can be used in networks other than the disclosing provider's network. The desired end result of designing an interconnection to the proposed template specifications is to maximize the performance, security, and safety of a service delivered to an end user.

A recommended Network-to-CPE Interconnection template is located at the end of Section 7.4. This template may further serve as the basis for development of a test suite for verifying interoperability.

Types of interconnections, but not necessarily all, that are covered by this template are listed below:

Information Services
Interactive Computer Services

Voice Messaging
Internet
Private Networks
Individual Consumers
Alarm Services
Electronic Publishing
Telemessaging

The key source that the proposed Network-to-CPE Interconnection template has been drawn from is the "Network Interface Specifications" template developed in the NRC II "Increased Interconnection Task Group 2 Report" (NRC II "The Path Forward"). The proposed Network-to-CPE Interconnection Template is a modification of this template that provides a focus on the user. The majority of content in the NRC II template has been maintained in the proposed Network-to-CPE template since it already does an adequate job of covering interconnection issues.

It should be noted that the Standards-Setting Group (FG2) is also drawing from the same template to identify the minimum list of items that should be addressed by standards bodies when developing interconnection standards (Section 9.2). This suggests that FG2 recommendations on standards development are closely tracking with the guidelines set forth in the proposed Network-to-CPE Interconnection template.

NETWORK-TO-CPE INTERCONNECTION SPECIFICATION TEMPLATE

Interface Specification Criteria	Check off
Service Demarcation : Establish a clear physical demarcation point between the network provider and the user that allows for signal loopback that isolates problems to either the network provider or the user side of an interconnection.	
Operating Environment: Define the physical operating requirements (temperature, humidity, premises access, *etc.*) to maintain equipment security and reliability in order to minimize interconnection disruption due to changing environmental conditions.	
Power and Grounding: Develop requirements that protect equipment from damaging power surges and anomalies, such as lightning, and that also ensure user safety.	
Network Survivability: Define level of service survivability in terms of network route diversity and equipment redundancy in accordance with the criticality of the interconnection.	
Interference Tolerances: Define protection levels relative to radiated and conductive electromagnetic properties of equipment and facilities in order to mitigate signal interference.	
RF Transmission Specifications:	

Define frequencies, channelization, bandwidth, power level tolerances, adjacent channel interference levels, *etc.*, for interconnections using RF media, such as over the airwaves or via coaxial cable.	
Transmission Specifications: Define network interface performance objectives in terms of signal transport time (delay), availability (downtime), lost message probability, transmission criteria (signal levels, signal thresholds, BER, loss, noise, phase jitter), *etc*..	
Protocols: Define data communications protocols and level of conformance to the seven layer model OSI protocol stack to ensure interoperability between network provider and user devices.	

Message Set: Define data communications message set that will be transmitted across the network provider/user interface to ensure interoperability.	
Network Security: Develop gateway screening functional requirements to block accidental or intentional intrusion of unwanted/inappropriate messages/commands.	
Fault Mitigation: Define error correction techniques, re-transmission overload controls, and other mitigation criteria that prevent fault migration through the network.	
System Diagnostics: Define requirements for fault detection, identification, and correction in the network to expedite maintenance procedures.	
Network Synchronization: Define synchronization and timing requirements, including source and stratum level of timing and availability of back-up timing to minimize accumulated jitter and wander and the occurrence of timing slips that cause the loss of user data.	
Transition Management: Ensure forward and backward compatibility of upgrades to equipment, including protocols and other features/functions, to minimize service disruption and cost impacts to users.	
Network Management: Define local and remote network management capabilities, including monitoring, provisioning, and level of access and control of the interconnection by the user.	
Performance Monitoring: Define the performance parameters that will be tracked by the Network Management system to provide proactive maintenance of the interconnection.	
Testing: Define both intrusive and non-intrusive test capabilities and identify the test access points for the purposes of fault isolation.	

7.5 DEFINITION OF "ADEQUATE" STANDARDS FOR VENDOR COMPATIBILITY

Introduction

This section identifies the issues and proposes recommendations to achieve "Adequate" standards for vendor compatibility to work towards the goal of seamless interoperability of telecommunications equipment, networks and services.

In this context, an “Adequate” standard for vendor compatibility is defined as a specification in which an equipment, service or network is detailed in such a way as to provide a basis for a consistent, vendor-independent interoperable implementation. This implementation would provide a basic level of operation upon which additional options or services may be provided. As sophistication of the products increases, some features and options may evolve into specification requirements.

When introducing new services, the basic level of operation is appropriate as part of the National Services component of the Services Planning Process Model of Section 4.2 of this report. In the past, the 1-800 number and the Caller ID schemes would fall into this category. The 'additional options level' would correspond more closely with the Regional Service Deployment component of the Model. In this case, vendors seeking interoperability between the competing products would need to agree on the interoperability of optional features.

The "Adequate" standards definition is dependent on how a particular product is connected. CPE may be required to deal with several categories of connection requirements. These include asynchronous, start-stop method of transmission; synchronous transmission, which requires careful synchronization through the use of highly accurate clocking devices; or isochronous transmission of synchronous data without the use of a clocking source. The transmission category may not be the same for both CPEs intended to interoperate. In addition, various compression schemes may be used in the inteconnecting network systems. Data such as voice can be compressed in the network without serious degradation of the service. However, data, such as video, that requires timed delivery, cannot be subjected to network compression.

The use of the varied transmission categories and compression schemes is essential in order to allow innovation. An example where diverse technologies are contributing to innovation is the evolving technology for connection of voice over the Internet. Manufacturers should build products that are designed to operate with one or more of the connection categories. To ensure interoperability for each connection category, there should be one common set of conformance and interoperability tests defined.

The degree of optional feature interoperability is an important consideration. This can be illustrated using an example. Most companies support some sort of compression in their CPE. To ensure interoperability, the user equipment must implement the same compression algorithm at both ends of the connection. In the case of ISDN, STAC compression is common. If the basic goal is to provide connection between units, then meeting the connection category standard would achieve this goal and the requirements of the basic level of operation. To enhance the product, a manufacturer may, in addition to the basic level of operation, chose to provide his own proprietary version of compression which is more effective. This could eventually supplant the standard and establish a de facto standard. In this example, the requirement of competitiveness, innovation and interoperability are all met simultaneously.
Within the CPE industry, standards exist which are recognized by the vendors. "Seamless interoperability" can only be achieved through testing of all product components for conformance to these standards and demonstrating that they all work in concert. This can be done through a

form of testing that allows manufacturers to work together in a low profile, low risk environment.

Data Collection

The information which is summarized under Key Learnings and which contributed to the formulation of Recommendations in this section is based on extensive work in ISO/IEC JTC1 and its Sub-Committees as well as the ITU-T Study Group 7 (Data Networks and Open Systems Communications), Study Group 10 (Languages for Telecommunication Applications) and Study Group 11 (Switching and Signaling). In addition, members of the North American Interoperability Policy Council were consulted. These members include representatives of the Information Technology Industry (ITI) Council, National Institute of Standards and Technology (NIST), the American National Standards Institute (ANSI) and the Telecommunications Standards Advisory Council of Canada (TSACC).

7.5.1 Key Learnings

Key Learning 1

In many cases, standards corresponding to the interfaces at which interoperability is required are not identified and are not publicly available. Systems are being designed according to private specifications, regional requirements, forum and consortia agreements, as well as international standards. The same standards and specifications are not available to all manufacturers and vendors.

Those in the telecommunications industry must be aware of existing standards and know how to apply them. Most standards are written in generic form and may be subject to different interpretations. Well written standards are precise and unambiguous and clearly state their scope and field of application.

A standard often points to other standards in order to specify related detail and avoid reproducing the content from another standard. This is to simplify version control and revision of interrelated standards. This, however, complicates the implementation process and increases the probability of implementation error.

CPE manufacturers build products to different sets of standards, a set of standards required to interconnect with the public network as described by the Open Systems Interconnectivity (OSI) model, for example, and also standards that allow products to interoperate with each other. The second set of standards are those required to make products interoperate with each other. The standards involved may be defined by the ITU-T, IEEE, the Internet Engineering Task Force (IETF), and others. Some telecommunications standards are well defined and stable while other standards are rapidly evolving. In many cases, by the time a standard is completely developed, a successor standard is under development. This is a moving target. The driving force behind this rapid evolution is the changing customer requirements. The standards serve as the foundation

upon which new capabilities are developed. Success for a company depends on its ability to understand and respond to new requirements in a timely manner.

Key Learning 2

Currently, standards for communications products and services include many options. If the options are chosen differently by different manufacturers, their products may not interwork. Some standards include options to accommodate more than one solution to the same problem in order to reach consensus. Such options should be avoided if possible. Other options are included to allow new features to permit competition and innovation.

The development of new features and options are determined through customer requirements. Manufacturers often are flexible in their system designs to allow for the addition of new options. The evolution of the enterprise network requires manufacturers to collaborate in some situations where competing products are working together. Such collaboration often leads to the definition of standardized approaches.

It is difficult to define up front what the new capabilities might be. Based on features offered by several manufacturers, the customers will choose the best option for their needs. The competitive environment in this case is evident. In some cases there may be more than one choice but no single choice fully satisfactory to all . In such cases it may be best not to define a standard. Instead, it may be to the benefit of all parties if the manufacturer develops implementation code and makes it publicly available. This would allow all other manufacturers to build interoperable products also and benefit the end user. The originating manufacturer would have the advantage of earlier time to market.

In some situations involving competing approaches, manufacturers may come to an agreement to support one approach over another. This usually depends on how the options are defined and how well they can interoperate with the various products. In most cases the option that takes the more universal approach is more likely be widely adopted.

7.5.2 Recommendations

7.5.2.1 The NRIC recommends to vendors that, for each interface their product lines support and at which interoperability is required, the interface specifications should be made publicly available, although such interfaces need not necessarily be standardized. However, where strict interoperability is essential, vendors should work together with TIA engineering committees and Committee T1 in order to choose from the existing standards or develop new standards to specify such interfaces. Once defined, such standards and the corresponding interfaces should be made publicly available. All relevant standards should be made easier to obtain and use. Further discussions of standards can be found in Section 9 of this report.

7.5.2.2 For national services, a basic level of connectivity must be ensured for each CPE. (See Section 4.) For more local services, competitive features, additional to the basic level of connectivity may be allowed. The NRIC encourages vendors to work with TIA engineering

Committees and Committee T1 to develop standards which ensure that each interface provides a basic level of connectivity and interoperability. At this level, the associated standard should be as simple as possible, allow no options and be based on the best available technical solution. Beyond this basic level, options to accommodate new features for the purpose of competition and innovation can be allowed. If vendors are to provide interoperability at this higher level, they would need to agree among themselves on a common set of features and tests, and specify the additional conditions for interoperability.

7.6 AIN AND NETWORK TO USER INTEROPERABILITY

The Advanced Intelligent Network (AIN) is an evolving, service-independent network architecture that provides important new capabilities for the rapid creation of customizable telecommunications services. Examples of services currently supported by AIN include 800 services, PCS, and local number portability.

This Statement of Issues identifies the engineering and other technical barriers to network accessibility and interoperability that are associated with the Advanced Intelligent Network (AIN) architecture and are in the domain of the User to public network interface. At the direction of the NRIC, a review of the prior work of the Network Reliability Council has been made to determine whether those findings have adequately identified barriers to the interconnection and accessibility to networks by CPE and other User interfaces such as private networks. This review considers whether those findings and recommendations are adequate to avoid barriers to network interconnection and accessibility in the reasonably foreseeable future.

The NRIC has also asked that when the recommendations are not adequate, additional or expanded recommendations to avoid barriers to network interconnection and accessibility by Users be developed. In particular, Focus Group 1 should recommend a process, or processes, to avoid barriers.

By following these recommendations third party providers will be able to interconnect and deploy new AIN services while maintaining the integrity of the core network.

SCOPE

A review has been made of the NRC’s "Network Reliability: The Path Forward, A Compendium of Technical Papers," April, 1996. The review was limited to Section 3, "Reliability Concerns Arising from Changing Technologies." The review was further limited to the Advanced Intelligent Network Subteam Final Report (February 22, 1996). The barriers identified below were described in Section 5, "Study Results Key Learnings Recommendations." The relevant sections were found to be (5.4) "Service Creation/Provisioning Process," (5.5) "Interoperability," (5.6) "AIN Network Overload Controls and SCP Capacity and Overload," (5.8) "SSP/SCP Testing," and (5.9) "Emerging Challenges - AIN Interconnection."

The recommendations of the NRC-2 report with respect to AIN Interoperability are comprehensive and adequately address the issues in relation to NRIC Focus Group 1.

7.6.1 Key Learnings

7.6.1.1 Service Creation/Provisioning Process

Poor service logic design can be introduced through new translations, improper provisioning of parameters, or AIN feature interactions. As a result, AIN services with central office-wide triggers and possibly line-based triggers could cause severe outages (*e.g.,* 800 Service). The Subteam Final Report expected most triggers to remain limited to individual lines or subscribers; however, telecommunications carriers have indicated that office-wide triggers are in use.

The recommendations of the Subteam Final Report for handling this problem are adequate. They are based on the service provider's implementation of a service creation/provisioning process to ensure the quality of the AIN services and maintain the integrity of public networks. This process includes testing between the developed application and the switched networks (including SSPs, SCPs, IPs, and STPs). Special consideration should be given to failure conditions and customer notification and control during network or service failure.

Providers of AIN-based services will need access to appropriate laboratory facilities (with sufficient public network simulation). The IITC is a suitable environment for this need. Because of the service provider's ability to create applications with AIN, this testing will at times need to be conducted in a coordinated fashion with network equipment suppliers and service providers.

7.6.1.2 Increased Interoperability

As interconnection increases, feature interaction between the public networks and Users (particularly private networks) will be more difficult to detect and prevent. As interoperability increases, capacity management will become more difficult. For example, private networks, when connected to public networks, may be overloaded by the intensity of access requested.

The recommendations of the Subteam Final Report are adequate. The Subteam Final Report recommends the use of processes and procedures for reliable interconnection, interoperability, and operation that must be met before interconnection is allowed. Reference should be made to the Network to Network Implementation Task Group of Focus Group 1 interconnection checklist. This template will be maintained by the NIIF. Telecommunications carriers should work together or through Committee T1 to develop interconnection standards for AIN service interconnection and AIN network interconnection for the multi-service provider environment.

7.6.1.3 Interoperability

As interconnection increases, service protection firewalls and confidentiality will be more difficult to maintain. The recommendations of the Subteam Final Report are adequate. Again, they recommend the use of processes and procedures for reliable interconnection, interoperability, and operation that must be met before interconnection is allowed. Bellcore's GR-1469-CORE, "Security for OSI-Based TMN Interfaces," Section 4 (Security Services), Section 5 (Security Mechanisms), Section 7 (Security Requirements for the OSI-Based TMN Interfaces) should be followed when applicable.

7.6.1.4 AIN Network Overload Controls and SCP Capacity and Overload

AIN service capabilities introduce the possibility of causing SCP overload. Existing AIN congestion control features are questionable in terms of their effectiveness to handle the increasing volumes of AIN service activity.

The Subteam Final Report provides several recommendations surrounding the use of supplier's employment and provision of forecasting models, the network provider's use of load testing, the SCP supplier's development of an improved automatic congestion control mechanism, and the NIIF's continuation of its efforts to establish industry alignment on Call Gapping and Automatic Congestion Control implementation. It is expected that the Network to Network-dedicated Task Groups of Focus Group 1 are reviewing these recommendations. For the Network to User Interoperability Task Group, special emphasis should be placed on the Report's recommendation that AIN service providers (which may be Users) understand and follow SCP engineering practices provided by the SCP vendor.

7.6.1.5 SSP/SCP Testing

SSP/SCP testing should be improved. The implication of AIN and, more specifically, the open call model (Ref. Bellcore GR-1298 and ITU's CS-1R), is that there exists a virtually infinite number of possible test cases. A complete test of every possible permutation of related parameters is not practical with the current state of software and system testing technologies.

The Subteam Final Report recommended that a standardized interface simulator be developed and used by companies conducting AIN testing, and that a standardized suite of test cases for each network element be developed and maintained. The suggestion was offered by the Subteam that ATIS, Bellcore or the TIA be considered as sources for this work. If the industry does not endorse a standard simulator, then each company conducting AIN testing will need to use some other type of interface simulator that adequately represents real network conditions.

7.6.1.6 Mediation and Third Party Service Provider Access

The provision of alternative services by third-party service providers may challenge the existing service functionality and network reliability. There are two specific areas of concern that need to be addressed. The first is mediation.

Earlier NRC work has defined mediation, or mediated access, as the set of real time and/or non-real time functions needed to facilitate secure, cost-effective third party access to local and other service provider AIN capabilities that will foster the open evolution of, and competition in, the local exchange network and other networks.

Mediation concerns both network protection and third party service provider access. Network protection includes screening, authentication, performance monitoring, fault management, and network traffic management. Third party provider concerns include the subjects of routing, recording, billing, provisioning, maintenance, and service/failure interaction resolution. LEC service providers have expressed concerns that, from an architectural basis, AIN has not been designed to readily accommodate third party service provider access and that additional forms of mediated functionality are required to support third party AIN access. The concerns of third party service providers include the timely availability of AIN functionality (in a competitive environment), network reliability, and duplication of existing network mediation capabilities.

The evolution of AIN technology must be guided jointly by the LEC, other network providers and third party service providers so as to allow an agreement on the type of third party access needed, what mediation functions are needed, the level of mediation needed, and the placement of mediation functionality in the network. Previous NRC work has described trigger access as the process of identifying calls that need AIN handling. When an AIN switch encounters a trigger, normal call processing is suspended and a query is launched to the SCP. The subsequent SCP response indicates how the SSP should continue processing the call. Triggers may include off-hook delays, originating no answer, and terminating busy dispositions. Access to AIN triggers suggests that local service provider switching equipment is capable of appropriate trigger detection. In addition, the local service provider must support a third party service provider's use of these triggers for call control in support of features and services. Other issues that must be resolved for effective third party trigger access include the designation of the responsibility for assigning triggers and maintaining records, determination of whether a third party service provider will be allowed to provision triggers in the LEC's switching equipment on behalf of their end customers, and determination of the operations support systems that will be available to third party service providers in support of maintaining their assigned triggers.

The Subteam's recommendations provide a good basis for resolving these issues. These recommendations include consideration of both the third party service provider's needs, and the telecommunications industry's goal of maintaining network integrity and reliability. As networks become more complex and interconnected, and there are an increased number of triggers offered, additional mediation functions will be needed.

Several industry bodies are currently addressing these issues. They include: the NIIF (an ATIS forum) and Bellcore.

7.6.2 Recommendations

The recommendations of the Subteam Final Report should be followed as indicated above. The specific recommendations can be found in the February 22, 1996 "Network Reliability Council

(NRC), Reliability Issues - Changing Technologies Focus Group, Advanced Intelligent Network Subteam Final Report." This report can be found on the World Wide Web at the site: http://www.fcc.gov/nrc/fg3/2ain.doc.

The following are the specific references to the recommendations referred above:

- Service Creation/Provisioning Process, Section 5.4 < Recommendation 18 >
- Interoperability, Section 5.5 < Recommendations 19, 20 >
- AIN Network Overload Controls and SCP Capacity and Overload, Section 5.6 < Recommendations 21,22, 23, 24 >
- SSP/SCP Testing, Section 5.8 < Recommendations 26, 27 >
- Mediation & Third Party Service Provider Access, Section 5.9 < Recommendations 28, 29 >

8.0 INTERNET INTERCONNECTIONS

8.1 STUDY PROCESS

During the early stages of the study process for User Interoperability, the NRIC Steering Committee requested that special attention be paid to interconnections between Internet Service Providers (ISPs) and telecommunications carriers. This section was created to bring greater visibility to the issues. The task group gathered information from practitioners in the Internet Service Provider industry, the telecommunications carrier industry, and equipment manufacturers.

8.2 KEY LEARNINGS

The fundamental issue identified, and woven through all the other issues in this section, is that the volume of Internet usage in the country has reached the level where the operators of the Public Switched Telephone Network (PSTN) and the ISPs must engage in effective joint planning to deliver their services efficiently. Bell Atlantic, for example, reports that ISPs create demand equal to about one-third of that of the interexchange carrier demand. The US telecommunications environment has become a network of telecommunications carrier networks which are interconnected in a variety of ways to other user networks, at varying degrees of efficiency. It is to the combined benefit of the telecommunications carriers and the ISPs to jointly address these issues so that the US economy can continue to thrive as a world leader in this arena.[41]

Issue: Planning and Notification

Successful implementation of interconnections between ISPs and the PSTN require an exchange of information relating to changes in demand, usage profiles and technologies. Demand for Internet and Information Service access has grown at levels that surprised both telecommunications carriers and the ISPs.

Issue: Physical Interconnection Options

Enhanced Services Providers (ESPs) have traditionally interconnected to the PSTN by means of circuit-mode mechanisms, such as Measured Business Lines (via analog copper pairs), multiplexed DS1s, Feature Group B trunks (950 service), Feature Group D trunks (1-800 service), ISDN Basic Rate Interface (BRI) and ISDN Primary Rate Interface (PRI). As usage of the Internet increases, other interconnection techniques may allow the development of more services, with higher performance, and possibly at lower cost. Section 7.2 discusses some of the end user issues related to the introduction of higher speed technologies and connections.

[41] ISPs are organizing to address operational problems arising on the Internet; for example, IOPS.ORG was formed in May of 1997.

A number of new technologies are emerging for making the connection between the customer premises and the PSTN. These include: Digital Subscriber Line (xDSL), Cable TV systems and Wireless. However, the mechanisms for connecting from the PSTN Central Office to ISPs have not changed materially since the emergence of ESPs.

Issue: Protocol Interconnection Options

When networks are interconnected, a variety of information needs to be exchanged to indicate characteristics of data traversing the interconnection. These data may address traffic priority, Quality of Service (QoS) requirements, and toll information. As is the case with Signaling System 7 (SS7) in the PSTN, it is beneficial to specify such standards at the point of interconnection between the PSTN and Internet, as well as among ISPs.

Issue: Fault Isolation

Both ISPs and telecommunication carriers are called by their customers when problems occur. The source of the problem may be within the ISP's plant, the PSTN, or devices and software owned by the ISP customer. It is therefore useful to share element performance information between the PSTN, the ISP network, and the customer. Additional fault isolation issues for end users, as a result of increased interconnections, are discussed in more detail in section 7.

Issue: Joint Efficiency

Engineering issues cannot be easily separated from competitive economic issues. There is consensus within this team, however, that end users will drive the competitive forces to deliver a broad range of services at a broad range of prices, possibly including price/performance services related to service access and reliability. While the development of a data-friendly local network is beneficial to all parties, the task group acknowledges the significant potential advantages created by allowing competitors to differentiate services based on a variety of functional, performance and value variables. For example, some ISPs create differentiation based on the local configuration, quantity and features of the local modem plants and access servers. Telecommunications carriers can differentiate their offerings with a variety of interconnection options to both end users and ISPs

8.3 RECOMMENDATIONS

8.3.1 ISPs and telecommunications carriers should establish a performance measurement program to assess and monitor the interconnections between the PSTN and ISPs.

Rather than relying on anecdotal evidence to evaluate the impact of ISPs on the PSTN and visa versa, it would be beneficial to end users requiring network reliability and service stability if the ISPs and telecommunications carriers work together to establish statistically valid and standardized measurements of performance at interconnection points. This could include

measures such as calls blocked at the terminating switch, calls blocked at the inter-office trunk level, and dial tone delay. A template is described in section 8.4 which could serve as the basis for establishing such measures.

It should be noted that telecommunications carriers currently have no economic basis for treating ISPs differently than any other end user requesting similar services or interconnections. This team reviewed a number of proceedings and in fact determined that in some cases telecommunications carriers were specifically not allowed to offer special treatment to ISPs. If it is determined ISPs and telecommunications carriers are not able to work together to establish standard measurements and carry out joint planning, the FCC may consider whether ISPs constitute a special class of end user which should receive treatment or services not available to non-ISP end users. The FCC would need to define precisely the characteristics that define an ISP and possibly create some kind of registration process for ISPs which meet the commission's criteria.

8.3.2 ISPs and telecommunications carriers should develop protocol standards for the exchange of control and accounting information in a standardized and reliable way.

While the Telecommunications carriers can exchange control and toll information with Signaling System 7 (SS7), and X.25 data network can exchange similar information with the X.75 protocol, there is no comparable protocol within the family of Internet Protocols (IP). Likewise, there are few mechanisms for exchange of information between the PSTN and ISP networks. For example, it could be useful for the PSTN to pass Call Waiting signals to an ISP when the caller's line is active on the ISP network, but another call is presented. The ISP could notify the user that another call is pending, and perhaps cause the data session to be suspended while the new call is answered.2

8.3.3 ISPs and telecommunications carriers should develop mutually beneficial network management interface standards such that both PSTN and ISP network operators can monitor the performance of appropriate elements of each other's networks.

For example, it is useful for an ISP to see when a PSTN switch is experiencing blocking that prevents callers from getting to the ISP network. In the same way, the operator of one IP network (who may also be a PSTN operator) would benefit from knowing when an interconnecting network is experiencing congesting and dropping packets. In both cases, the network operators can take action to alleviate the problem caused by the network rather than spending time trying to identify whether a problem is within or outside their own network, and, more importantly, keep their customers informed of the cause and restoration plan. Section 6, "Operations," describes the issues and recommendations for a Gateway function more fully.

8.4 INTERNET INTERCONNECTION SPECIFICATION TEMPLATE

A crucial step in eliminating barriers to Internet interoperability is to establish a document that clearly and precisely defines the technical criteria and standards to be met by network providers and ISPs when providing a network to user interconnection. A requirements template has been developed that serves as a guideline for Internet interconnection. This template categorizes and briefly describes the technical specifications necessary to connect networks to ISPs. This template includes a checklist of technical areas-of-concern that must be addressed for each type of Internet interconnection to ensure interoperability. Addressing each technical category in the template by identifying specific interconnection specifications will ensure that a baseline level of interoperability will be achieved. This template may further serve as the basis for development of a test suite for verifying interoperability.

The template should be used by the network provider and the ISP to furnish as much relevant and detailed information as possible so that they may both deploy the appropriate equipment and services needed to meet interconnection requirements in a timely manner.

INTERNET INTERCONNECTION SPECIFICATION TEMPLATE

Interface Specification Criteria	Check off
Service Procurement Criteria	
Define Reasonable Planning Cycle Identify planning cycle that meets the needs of the ISP to forecast growth and the needs of the network provider to forecast service changes.	
ISP Usage Requirements Define expected usage by ISP location for the planning cycle (total number of minutes per month, number of minutes in the busy hour, identification of the busy hour, number of lines needed by type of service, *etc.*).	
PSTN Retail Service Availability Define retail services available (1MB Service, ISDN PRI Service, AIN features, Modem/PAD services., *etc.*) by Central Office for the planning cycle.	
PSTN Wholesale Service Availability Define wholesale services available, including bundled and unbundled wholesale services, for the planning cycle.	
Procurement and Identification of Network Services for ISPs Define standard procedures to order facilities that can be automated by both ISPs and network providers and that can be reconciled by both ISPs and network providers.	
Maintenance and Operations Criteria	
Fault Isolation Define procedures to insure that faults can be identified and corrected as quickly as possible and that communications of the process is shared between the network provider and the ISP.	

Operations Standards Implement procedures to share operational information related to performance of ISP lines	
Performance Measurements Implement ongoing performance measurements for offices that contain ISP lines that provide information on call blocking, dial tone blocking and implement ongoing performance measurements for ISP lines that identify percent redials.	
Performance Standards Create standards for ISP lines regarding percent redials and for offices that contain ISP lines for call blocking and dial tone blocking.	
Planning and Information Sharing	
Define Planning Cycle Identify planning cycle for information sharing that provides a long enough time frame to work out industry problems and provides information that can be forecast reasonably accurately.	
PSTN Changes to Local Dialing Areas Share proposed changes to calling area numbering and placement of equipment.	
ISP Long Term Growth Projections Provide information on seasonal growth patterns and expected service changes that may impact growth.	
PSTN New Service Deployment Plans Provide information on proposed new retail and wholesale services, including proposed tariff changes, deployment plans and protocol impacts.	

9. STANDARDS DEVELOPMENT PROCESS

Congress has specifically urged federal agencies to use voluntary consensus standards in their regulatory and procurement missions. This has been done in a number of pieces of legislation addressing specific sectors such as health care and fasteners. In addition, the National Technology Transfer and Advancement Act (NTTAA) provides overall guidance to federal agencies. Other recent legislation relying on voluntary consensus standards and limiting the Federal Communications Commission's (FCC's) role to one of oversight is the Communications Assistance for Law Enforcement Act (CALEA). This act clearly endorses voluntary industry standards and has FCC oversight involvement only in the event that a complaint is filed with the Commission claiming the industry standard is deficient under CALEA.

Section 256 of the Telecommunications Act of 1996 (TA96) does not specifically "require" the FCC to set up any oversight mechanism to monitor standards activities; rather the Section specifically uses the term "may," indicating the decision rests with the Commission. Thus, there is no requirement for the FCC to set up any new oversight mechanism related to Standards Developers (SDs) due to Section 256. However, the FCC has always exercised some oversight of standards creation activities, has frequently participated in standards work (as encouraged by the NTTAA and in the Office of Management and Budget (OMB) Circular A-119), has corresponded with technical experts in various SDs, and has used standards material to assist in FCC regulations.

Interactions between SDs and the FCC have been effective, for example:

1) The FCC staff frequently confers with Telecommunications Industry Association (TIA) technical experts in TR-41.9 on technical issues arising under Part 68 and harmonization with Canadian requirements in CS03, and FCC staff directly participated in the development of TIA/EIA-631 to address electromagnetic compatibility (EMC) concerns with terminal equipment.

2) The Joint Technical Committee (JTC) formed by T1P1 of Committee T1 and TR-46.3 of TIA produced air interface standards for the 2 GHz PCS band, and an overall Program Management Plan which identified needed standards, the likely developers, and schedules. The leadership of Committee T1 (Committee T1 Chair, T1P1 Chair, and Committee T1's JTC Chair) met on several occasions with representatives of the FCC to share information on JTC planning and progress. One significant item of input from the FCC representatives was that they wanted stable technical specifications for the air interfaces to be available to bidders prior to the FCC spectrum auctions. This message was brought back to the JTC which adjusted its program and met this goal. Three of the air interface draft standards were sent out for ballot prior to the auction and the other three shortly after that. Approved standards were not available prior to the auction, but stable text in draft standards was available from Committee T1 and TIA, prior to the auction, for all the technologies. This was publicized in a joint Committee T1/TIA press conference so all

potential bidders would have access to the information. In this way the JTC was able to meet the FCC request. The communication channels between the FCC and the JTC were informal, but were effective in keeping both parties aware of the activities and expectations.

3) TIA standards for analog cellular were used by the FCC as a way of ensuring interoperability of handsets and use across both systems in the A and B block. TIA standards have also been adopted by the FCC as part of Part 68 to ensure Hearing Aid Compatibility (68.316).

4) The FCC referred to Committee T1 in its 1996 Order in CC Docket No. 93-268 amending Part 68 to include equipment standards for connecting customer provided terminals to the Integrated Services Digital Network feature of the public switched network. This order was addressed by the reissue of the Committee T1 Technical Report Number 05.

5) The FCC has referred to TIA and the Institute of Electrical and Electronics Engineers (IEEE) standards in the Commission's recent Order in CC Docket No. 87-124 requiring volume control on all new wired telephones and cordless telephones. The FCC has used IEEE standards as guidance documents for environmental regulations enforcing the National Environmental Policy Act (NEPA) related to human exposure to radio frequency energy. TIA Telecommunications Systems Bulletins (TSBs) have also been used as guidance for interference studies on point to point microwave systems (TSB-10-F) as well as testing under Part 68 (TSB-31-A).

9.1 CHANGES NEEDED IN SECTION 6 (TECHNICAL STANDARDS DEVELOPMENT PROCESS ADEQUACY ASSESSMENT) OF THE RECOMMENDATIONS OF THE INCREASED INTERCONNECTION TASK GROUP OF NRC II TO BETTER MEET THE NEEDS OF THE TELECOMMUNICATIONS ACT OF 1996

9.1.1 Key Learnings

While much of the information contained in Section 6 of the NRC II document forms a good basis for understanding the technical standards development process, a number of recommended revisions and updates have been made by NRIC Focus Group 2.

9.1.2 Recommendations

9.1.2.1 The Standards Development Process and Recommendations

As a result of their ANSI accreditation, the technical standards development processes for the TIA Engineering Committees and Committee T1 are similar. The complete standards life cycle process as viewed by Committee T1 follows.

STANDARDS LIFE CYCLE PROCESS

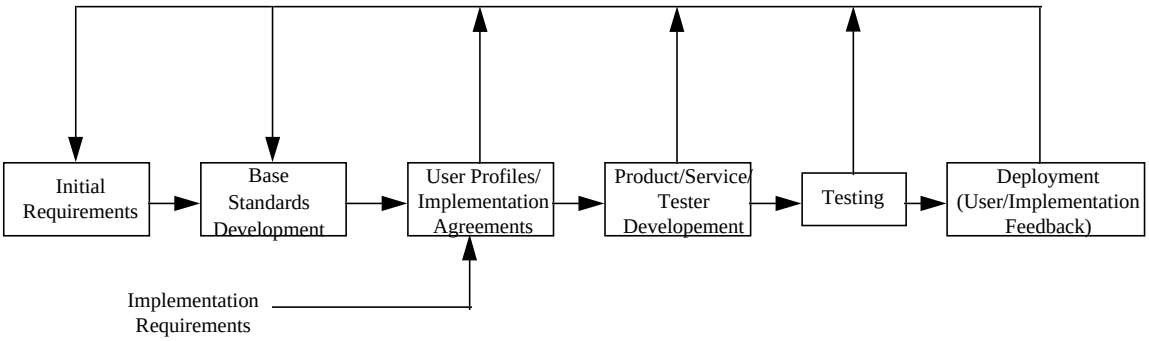


Figure 9.1 - Standards Life Cycle Process

The standards process is cyclic and so could theoretically start at any stage. In general, a flow beginning from the far left to the right, with feedback as shown, provides the most orderly introduction of a service or technology interface.

Stage 1: Initial Requirements. Inputs from users, manufacturers, network providers or service providers that can provide an initial, perhaps high-level, basis for defining the service capability or technology interface.

The initiation of the base standards development process is activated by a variety of sources. Listed here are some of them.

- Emergence of new technologies, *e.g.*, Personal Communications Services (PCS), Asynchronous Transfer Mode (ATM), Wavelength Division Multiplexing (WDM), may require new interfaces.
- Industry group(s) submit requirements to exploit a business opportunity.
- Network user requests for additional capabilities stimulate new features or enhancements
- Industry evolution causes necessary accommodation of new interfaces
- Regulatory/legislative action mandates new interconnection points or arrangements

Stage 2: Base Standards Development. A minimum set of requirements defining interoperability provides an opportunity for individual manufacturers and network/service providers to be innovative in providing additional features and performance capabilities while maintaining interoperability. This standards stage may require the cooperation of multiple organizations that develop standards within the U.S. (*e.g.,* Committee T1, TIA, Internet Engineering Task Force (IETF), IEEE and National Committee for Information Technology Standards (NCITS)) and harmonization with other standards bodies around the world. With regard to the latter, Committee T1 is the primary source of U.S. contributions to the International Telecommunication Union - Telecommunications Sector (ITU-T) through a U. S. State Department process. It originates more than 1,000 such contributions each year.

User and industry needs for reliable interoperability can be facilitated by the base standards development process that provides a comprehensive set of standards addressing the broad range of issues critical to interoperability. Program management techniques, including clear objectives, a customer involvement process, project milestones, identification of the dependencies between project elements and project tracking can focus standards work to provide timely outputs. Reliable interoperability can also be aided, in some cases, through performance requirements for network elements that are consistent with performance and protocol specifications at the network interface.

Recommendation 1

Use of a Network Interface Specification template is advised when a new network interface is identified for standardization. Standards bodies should use this type of template in developing the initial Standards Project Plan(s) for new interfaces to address the relevant important areas for interconnection reliability. An example template for standards development planning is contained in Section 9.2.

Implementation Target Date: Now, and continuing

Recommendation 2

Industry associations, such as ATIS and TIA, should consider the value of incorporating performance requirements for complex network elements with the interface standards requirements. Also, the associations should consider how such requirements should be developed and funded.

Implementation Target Date: Now

Stage 3: User Profile Implementation Agreements. Standards should be forward-looking and provide a target for the features a specific technology or service interface may develop. It is beneficial to identify how a new technology or service interface standard can be used with other standards to provide an application that meets a user's need. With new technologies or services it may be difficult to initially provide all capabilities ubiquitously. Therefore, it is essential that capabilities be prioritized to lead service capability requirements. Forums frequently facilitate this function by identifying priority user applications, and the profile of standards to provide that application, and by developing interconnection agreements of the key standardized features to implement in the technology/service interface introductions. New technology or service concepts that emerge in this process stimulate inputs to standards bodies.

Recommendation 3

Wherever appropriate, standards bodies should work with other industry groups that use standards, such as the ATM Forum, to more precisely define standards requirements and minimize complexity and optionality. Excessive optionality can be dealt with through an appropriate contribution to the affected standards committee or forum. A Network

Interface Specification, such as the example contained in Section 9.2 of this report, should also be used by industry forums to further define, detail and approve implementation for the industry.

Implementation Target Date: Now, and continuing

Stage 4: Product/Service/Tester Development. Individual companies develop products, services, network elements and test equipment based on standards. Since the standards are voluntary, these products/services may fully or partially comply with the standard. In addition, they may include features or capabilities beyond the base standards or the implementation agreements. These features and capabilities may provide a source of inputs to standards bodies.

Stage 5: Testing. Industry Testing (including interoperability testing) of telecommunications technologies can provide users and the industry with insight into characteristics (including interoperability between multivendor products) for a specific technology. Issues identified can be the basis for enhancements to the standards for that technology. Such testing is particularly important for widely deployed and critical network control technologies, *e.g.*, Common Channel Signaling (SS7).

Stage 6: Deployment (User implementation Feedback) Deployment of standardized telecommunication technology, service or network capabilities provides an opportunity for user needs to be satisfied and for practical experience with the network reliability of these capabilities. Feedback on introductory capabilities can stimulate needs for additional features and for improvements in standards to support new products, services and test equipment. This feedback is also important in the evaluation of the associated standards.

9.1.2.2 Standards Organizations

Within the U.S. telecommunications industry, Committee T1 and TIA have been the primary standards developers. The Society of Cable Telecommunications Engineers (SCTE), working on behalf of the cable television industry, will focus on "physical layer" standards for coaxial cable systems, while looking to Committee T1 and TIA groups to address other telecommunications needs. Other ANSI-accredited organizations such as the National Committee for Information Technology Standards (NCITS) and the Institute of Electrical and Electronics Engineers (IEEE) also develop standards that are used by the telecommunications industry ranging from methods of testing to determine attributes for electronic equipment such as telephone handsets to human exposure to radio frequency energy. IEEE also has done work for Radio Local Area Networks (RLANs).

In addition, a variety of forums, associations, task forces and committees also generate technical and other documents used within the industry. Examples of these include the ATM Forum, Carrier Liaison Committee (CLC), Internet Engineering Task Force (IETF), Network Management Forum (NMF), Satellite Broadcasting and Communications Association (SBCA), and Satellite Industry Association (SIA). Contact information for these organizations is included in Section 9.3.2. Many attempts have been made to identify all forums/consortia involved in the communications and information technology industries. One is a publication by Bellcore entitled

"Telecommunications Industry Catalog of Forums, Standards Bodies & Associations". Another is a report compiled by the Telecommunication Technology Committee (TTC) and presented at the Global Standardization Collaboration meeting in June 1995 in Ottawa, Canada (GSC 2), and updated at the GSC-3 meeting in Kyongju, Korea, September, 1996.

Telecommunications systems interoperability is not limited to national interests. International interconnection demands cooperation on standards, now well beyond that needed for simple voice telephony. The Global Information Infrastructure (GII) requires global telecommunications standards within such groups as the International Telecommunication Union (ITU) and increasing collaboration among the various national/regional standards bodies (*e.g.,* ETSI in Europe, TTC in Japan, Committee T1 and TIA in the U.S., TTA in Korea, ATSC in Australia, and TSACC in Canada). These organizations get together periodically to share information on high interest areas of mutual concern in a forum known as Global Standards Collaboration (GSC) and discuss radio standardization matters in a forum known as RAdio STandardization (RAST). In this hemisphere, standards coordination occurs both in the North American Free Trade Agreement (NAFTA) sponsored Consultative Committee Telecommunications (CCT) of which TIA is the USA Secretariat, and via the InterAmerican Telecommunications Commission (CITEL) of the Organization for American States. Committee T1 and TIA have been leaders in initiating harmonization and collaborative efforts.

9.1.2.2.1 TIA

TIA's eleven Engineering Committees are open to materially interested parties in accordance with TIA's ANSI-approved Engineering Manual. Voting participation on TIA engineering committees or subcommittees requires either being an active dues-paying member of TIA (dues range from $1,000 to $50,000 based on size) or paying a non-TIA-member participation fee. The non-member fee currently ranges from $1,000 to $10,000 yearly, depending on the work program and number of weeks of meetings the committee/subcommittee plans to hold and the resource needs of the Formulating Group. The Engineering Committees contain manufacturers, users and service providers (wireline and wireless), government agencies, and others interested in the work of TIA's Formulating Groups. Some Formulating Groups meet two weeks/year; some others meet as often as 15 to 16 weeks/year. TIA Engineering Committees also make contributions to the ITU via the Department of State in technical areas within the scope of the TIA formulating groups as well as contributions to the International Electrotechnical Commission (IEC), the International Organization for Standardization (ISO), and ISO/IEC Joint Technical Committee 1 on Information Technology (JTC-1). Information on TIA's technical programs can be found in TIA's Standards and Technology Annual Report (STAR). Copies of STAR as well as a complete listing of current projects numbers (PNs), Standard Proposals (SP) to ANSI for American National Standards, and a catalog of published documents can be found on TIA's web page at www.tiaonline.org. TIA document information can also be found on ANSI's National Standards System Network (NSSN).

9.1.2.2.2 Committee T1

The mission of the Committee T1 is to develop technical standards and reports supporting the interconnection and interoperability of telecommunications networks at interfaces with end-user systems, carriers, information and enhanced-service providers and customer premises equipment (CPE). The T1 Committee currently has six Technical Subcommittees that are advised and managed by the T1 Advisory Group (T1AG). Each recommends standards and develops technical reports in its area of expertise. The subcommittees also recommend positions on matters under consideration by other North American and international standards bodies. Committee T1 is the largest provider of U.S. contributions to the ITU (approximately 2000/year through the U.S. State Department process).

The Alliance for Telecommunications Industry Solutions (ATIS) sponsors and provides the secretariat support for Standards Committee T1. Additionally, the American National Standards Institute (ANSI) accredits Standards Committee T1.

Membership and full participation in Committee T1 and its Technical Subcommittees is open to all parties with a direct and material interest in the T1 process and activities. Free of dominance by any single interest, this open membership and balanced participation safeguards the integrity and efficiency of the standards formulation process. ANSI due process procedures further ensure fairness. Information on T1 activities, including in many cases draft standards, are available on T1's Web page (http://www.t1.org). Like TIA, T1 document information is also available on ANSI's NSSN.

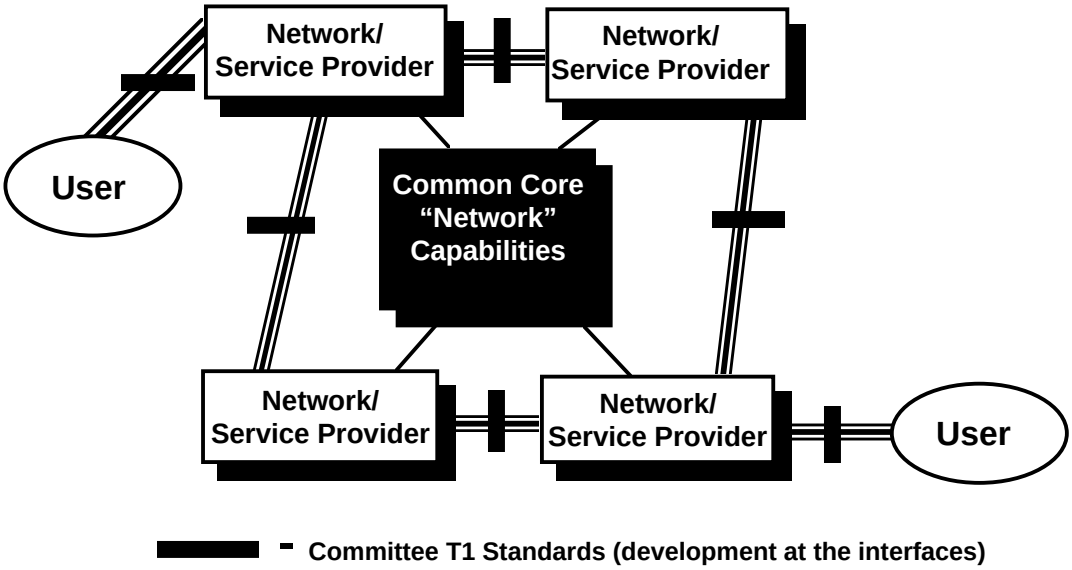


Figure 2: Sample Subset of U.S. Network of Networks, Committee T1 Standards

9.1.2.2.3 Internet Engineering Task Force

The Internet Engineering Task Force (IETF) operating under the auspices of the Internet Society (ISOC) has been the primary venue for the development of the Internet Protocol suite, its support protocols and the basic complement of applications operating over the Internet. The IETF is organized into eight areas, each managed by one or two Area Directors and consisting of up to 20 chartered working groups.

The Area Directors sitting as a body comprise the Internet Engineering Steering Group (IESG). A separate committee, the Internet Architecture Board (IAB) provides advice to the IETF, the IESG and the ISOC board of directors. Standards track technical specifications are normally developed in one of the approximately 90 working groups and forwarded to the IESG for review. Part of the IESG review includes a public comment period. Informational documents, documents that describe experimental technologies and standards track specifications approved by the IESG are published in a documentation series as RFCs (Requests for Comments). The IETF uses a three stage standards track process consisting of Proposed, Draft and Full Standards. There must be multiple interoperable implementations of a proposal in order for the technology to advance along the standards track.

Participation in IETF working groups, which do most of their work using electronic mailing lists, and attendance at the three times a year IETF meetings is open to all individuals. The fair and open procedures, defined in RFC 2026, ensure that IETF developed standards are of the highest quality, meet real needs and are not distorted by the influence of individual vendors.

9.1.2.3 Consortia

There is a cooperative relationship between telecommunications equipment suppliers, service providers and users. While competition exists among service providers and among suppliers for business in the same markets, a high level of cooperation is needed to achieve interoperability through standards. Success in creating a *de facto standard* by one or more companies to quickly achieve market presence is difficult since interconnection with user equipment and multiple networks in a multi-vendor environment is required. The need for backward compatibility and interoperability can create disincentives to de facto standards since such standards can create economic disadvantages and reliability problems for users, manufacturers and network providers.

However, there is concern that, as the industry evolves to respond to more competitive pressures, service providers may feel pressured to implement interfaces before standards are available. Often times a group of companies interested in pursuing a particular technology may join together to form a consortia to produce a statement of requirements or to create an actual technical specification. When such requirements are a precursor to standards work, the process is accelerated since a well-defined statement of user needs will assist standards groups in creating standards to meet those needs. In some cases the forums or consortia may begin to develop the technical document themselves when there is a perception that the traditional standards process is too slow. These types of activities raise questions of “openness” and “due process” and whether any essential intellectual property rights (IPR) such as essential patents will be available to all parties on reasonable and non-discriminatory terms. In other cases, consortia are formed to implement and/or promote particular standards by agreements directed to interconnection options

and deployment of networks based on particular standards. For example there are groups directed to promoting all 3 wireless technologies, Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA), and Time Division Multiple Access (TDMA).

Congress required, in Section 273 of TA96, that the FCC establish some minimum rules for certain non-accredited standards development organizations. The FCC has issued a Notice of Proposed Rulemaking in CC Docket No. 96-254 to establish these rules. Section 273(d)(4) prescribes procedures for "any entity that is not an accredited standards development organization and that establishes industry-wide standards for telecommunications equipment or customer premises equipment, or industry-wide generic network requirements for such equipment, or that certifies telecommunications equipment or customer premises equipment manufactured by an unaffiliated entity." Section 273(d)(4)(A) specifies the duties to which non-accredited standards development organizations are to adhere. These include such things as notice of new (or substantially modified) industry-wide standards or generic requirements, an opportunity to fund and participate in the work, a method for funders to provide comments on proposals, and dispute resolution methods.

In summary, given the many organizations involved in interconnection and thus contributing to a network of networks, network reliability can best be maintained if service providers follow the interconnection guidelines contained in this report.

Recommendation 4

New network providers are encouraged to participate in existing telecommunications industry standards processes, either directly or through associations, via membership or contributions to standards bodies, *e.g.*, Committee T1 or TIA.

Implementation Target Date: Now

Manufacturers benefit from participation in the standards and forum processes. System requirements and equipment specifications yield the opportunity to design, build and sell products to the network providers and telecommunications end users. However, if consensus develops slowly, manufacturers or service providers may be motivated to try to anticipate the standards. This can create a high risk opportunity to begin equipment fabrication before stable standards are available. In the mid-1980s this was the case for Basic Rate ISDN where the major U.S. switch manufacturers developed equipment based on two different technical specifications including different option selection (not a single standard). Later network requirements and components were changed to gain network interoperability.

As noted in the NRC II report, Committee T1 and TIA have both taken steps to speed up the time frame for the development of new standards. These improvements continue to evolve. Extensive use of Electronic Document Handling (EDH), electronic mail, web sites, electronic balloting, and other techniques are speeding up the process of standards development to meet competitive marketplace needs. For example, beginning in February 1997, all T1 ballots are now handled electronically.

Recommendation 5

Where adequate network interface standards exist, suppliers should develop and evolve their products to meet those standards. If interface standards are not yet established, network service providers and network equipment suppliers should be encouraged by the FCC to actively participate in the development of robust network interface standards to accelerate their availability.

Implementation Target Date: Now

Recommendation 6

Interconnecting network providers should utilize industry-proven interconnection standards.

Implementation Target Date: Now

Recommendation 7

While standards are generally voluntary, increased emphasis should be placed on the value of compliance in ensuring network interoperability and reliability. However, in the case of public safety concerns, standards are identified with a "mandatory" emphasis.

Implementation Target Date: Now

9.1.2.4 Timeliness of Standards Development

Experiences such as the pre-standard developments described in Section 9.1.2.3. and a greater market focus by U.S. telecommunications standards developers has dramatically improved the quality and timeliness of standards development. A few recent examples where timely standards development has been achieved in a *12 to 18 months* interval (from initial proposal or issue identification to stable standard) are:

Timely Standards Development Examples

Personal Communications Air Interface (approx. 8000 pages)	T1/TIA Joint Technical Committee (T1P1 and TR46.3)
PCS Mobility Management Application Program	T1S1 to meet TIA TR46 needs
Outage Index based on FCC-Reportable Outage Data	T1A1 for NRSC
SONET Directory Services	T1X1 and T1M1

Asymmetrical Digital Subscriber Line	T1E1 to meet market needs
ATM Adaptation Layer for Data, Signaling and Video Application (AAL.5)	T1S1 with input requirements from the ATM Forum
Lawfully Authorized Electronic Surveillance	TIA and T1 standard to implement CALEA
SS7 Protocol Enhancements and Architectural Analysis	T1S1 for NRC I

Standards groups such as TIA and T1 are continuously improving their processes to meet user and industry needs. For example, Exhibits 3 and 4 of the NRC II report described improvements that have been implemented in the last few years. Development such as the ANSI NSSN are providing access to standards information on a consolidated basis and ANSI is re-engineering its intervals to speed up the final ANSI approval and publication time for American National Standards. ANSI is beginning to direct its effort to the use of collaborative authoring programs and other aids to assist its accredited SDs in accelerating the development process itself. For example, templates are provided for use by a document editor to assist in putting the document in the correct format in the first instance. Electronic meetings and the use of information technology standards for the distribution of standards information are also being pursued by ANSI and its accredited SDs.

However, notwithstanding these efforts, broad concern still exists in the industry with respect to the ability of the standards process to keep pace with the accelerating requirements of new technology.

Recommendation 8

The most effective means to accelerate the standards development process is to ensure new standards work has sharp technical focus and clear standards deliverables, plus final and interim milestones for those deliverables. Exhibits 6 and 7 from NRC II contain information on standards project proposals and project tracking based on this recommendation.

Implementation Target Date: Now, and continuing

Recommendation 9

All telecommunications standards bodies, accredited and non-accredited SDs, should implement by year end 1997 interactive electronic access methods to expedite the submission, creation, acceptance, review and finalization of technical standards. This is already underway, but a completion date for all organizations has not been specified.

Implementation Target Date: Year End 1997

Recommendation 10

The Forum Process should be employed by the industry and companies/agencies to foster innovation and to produce contributions to the development of standards, not in lieu of standards. Industry forums have been instrumental in specifying implementation agreements.

Implementation Target Date: Now

9.1.2.5 Conclusions on Standards Adequacy

The voluntary, open, consensus-based standards process, including Industry Forums and Generic Requirements Process, is viewed as being adequate to support network interoperability and reliability issues relating to basic services on wireline and wireless networks. Congress, in the NTTAA, has specifically recommended the use of voluntary consensus standards to achieve the regulatory mission of federal agencies. OMB has proposed that independent commissions like the FCC, be included within the NTTAA's scope.

The industry survey data gathered for this report indicates a high degree of dependence on standards bodies to develop service, reliability and interoperability standards and specifications. However, the industry views standards bodies as having little responsibility for ensuring inter-network reliability and interoperability. Therefore, it is highly recommended that interconnecting network operators execute bilateral agreements and compatibility testing to ensure reliable interoperability. Groups such as the Inter-network Interoperability Test Coordination (IITC) were recommended by NRC II to assist in this effort. The data indicates a high level of support throughout the industry for the use of the standards process, industry forums, interoperability testing and bilateral agreements.

Quickly maturing and innovative standards development processes relating to cellular applications and interconnections with wireline networks are evident. The development or adaptation of interconnection standards for wireline and wireless networks with other networks, *i.e.,* cable television, some new satellite systems, and mobile satellite systems, is still in the future, although these efforts are being defined now.

Since 1984, the U.S. telecommunications network has grown, while introducing new technologies and services in a multi-vendor environment of more than 500 Interexchange Carriers, 1,500 Exchange Carriers and 1,000 Cellular service providers. The development by telecommunications standards bodies of working relationships with Industry Forums, a focus on the positive impact of the standards and continuous process improvements have allowed standards bodies to meet industry and user needs for timely standards development in the face of rapid evolution of technologies and the convergence of industries. Moreover, process improvements, including use of electronic document handling to facilitate and expedite standards development and dissemination, should ensure that the standards process can continue to improve to meet future challenges. In addition, the strategic impact of standards and increased executive awareness of the standards impact, where necessary, can stimulate corporate escalation processes for critical industry standards issues.

9.2 CHANGES NEEDED IN SECTION 5.6 (NETWORK INTERCONNECTION TEMPLATE) OF THE RECOMMENDATIONS OF THE INCREASED INTERCONNECTION TASK GROUP OF NRC II TO BETTER MEET THE NEEDS OF THE TELECOMMUNICATIONS ACT OF 1996

9.2.1 Key Learnings

The Standards-Setting Focus Group concurs with the NRC-2 Network Interconnection Focus Group 2 recommendation that the custodian of this template should be the Network Interconnection and Interoperability Forum (NIIF), sponsored by the Alliance for Telecommunications Industry Solutions (ATIS).

9.2.2 Recommendations

The following template has been modified from that originally developed by the NRC-2 Network Interconnection Focus Group 2. The original template was proposed by the NRC-2 Focus Group for a variety of uses including development of standards and definition of industry interconnection specification criteria. The template identified the minimum list of items to be addressed by a standards organization when developing a network interconnection standard.

Recommendation 1

The NRIC-3 Focus Group 2 on Standards-Setting, which is focused primarily on the process and roles of standards development organizations, recommends several modifications to the template. These modifications reflect the view that while all items listed in this template should be considered by affected service providers to establish and maintain interconnection, some items may not typically fall under the purview of standards-setting organizations. It should also be noted that other organizations may find the processes that evolve from this template useful and are encouraged to make use of and enhance it.

Implementation Target Date: Now

Network Interconnection Template

INTERFACE SPECIFICATION CRITERIA	CHECK OFF
[Define the physical/software interfaces in terms of existing tariffs and technical standards and government regulation.]	

Establish a clear point of demarcation that allows for non-intrusive test access.	
[Define the environmental operating requirements according to security and reliability needs.]	
[Develop power and grounding requirements in accordance with safety and protection regulations, codes and standards.] When applicable, develop power and grounding standards in accordance with safety and protection regulations and codes.	
Define network diversity requirements and survivability capabilities needed.	
Define interference generation protection levels relative to radiated and conductive electromagnetic properties.	
(Radio interfaces only) Define frequency channelization, bandwidth, power level, frequencies, tolerances and adjacent channel interference levels.	
Clearly identify protocol elements (*e.g.,* in terms of the seven layer model OSI protocol stack).	
Define all message sets that will be transmitted across the interface.	
Develop gateway screening functional requirements to block accidental or unauthorized intrusion of unwanted/inappropriate messages.	
Build for robustness by defining error correction, re-transmission overload controls and fault migration mitigation criteria.	
Develop message sets to facilitate fault detection, identification, diagnosis and correction.	
Develop network interface performance design objectives in terms of signal transport time (*e.g.,* delay), availability (*e.g.,* downtime), lost message probability and transmission criteria (*e.g.,* bit and block error rates, cell loss ratio, packet loss, noise, phase jitter)	
Define synchronization and timing requirements and establish monitoring and back-up capabilities.	

Ensure that forward and backward compatibility of the protocol is addressed for transition management.	
Provide local and remote network management notification and control capabilities.	
Develop a network impact statement to predict/specify the backward compatibility and purpose of the standard.	
Develop demonstrable performance criteria at agreed stages of specification development.	
[Define and conduct acceptance testing to validate the defined stages of specification development.]	

Brackets [] indicate items that may not be applicable to SDs.

9.3 CHANGES NEEDED IN SECTION 12, EXHIBIT 2 (KEY TELECOMMUNICATIONS-RELATED STANDARDS GROUPS) OF THE RECOMMENDATIONS OF THE INCREASED INTERCONNECTION TASK GROUP OF NRC II TO BETTER MEET THE NEEDS OF THE TELECOMMUNICATIONS ACT OF 1996

9.3.1 Key Learnings

The NRC II document Section 12, Exhibit 2, "Key Telecommunications Related Standards Groups", identifies a number of organizations involved in the standards setting process. However, additional standards bodies, forums, associations, *etc*., are actively involved in standards related activities. Information on these and other organizations can be obtained by searching the Internet, using keywords describing the organization, Key Area of Standardization, or Key Technology of interest.

9.3.2 Recommendations

Recommendation 1

It is recommended that the NRC II document Section 12, Exhibit 2, be re-titled "Key Telecommunications Standards Related Groups", and be modified as follows.

Implementation Target Date: Now

These changes expand the scope of organizations and the "technologies/focus areas" that are addressed and place them in concert with the larger scope of the NRIC. While, the ITU-T does

not normally address issues unique to the United States, ITU-T standards are often referenced in U. S. standards or used in the absence of U. S. standards.

This modified list does not identify every standards body, forum, or association dealing with telecommunications. It is solely intended as a guide to major standards related organizations involved in a majority of the technologies/focus areas that are relevant to TA96.

Key Telecommunications Standards Related Groups

	Key Areas of Standardization	Key Technologies/Focus Areas	Sponsor	Location/WWW	Contact (US) Phone Fax E-mail
Committee T1-Telecommunications **Committee T1**	Telecom Network Interfaces; Interoperability	BISDN, SS7, PCS, IN, TMN, SONET, Multimedia; Network Reliability, NII/GII	Alliance for Telecommunications Industry Solutions (ATIS)	Suite 500 1200 G St. NW Washington. DC 20005 http://www.t1.org/	Harold Daugherty 202 434-8830 202 347-7125 haroldd@atis.Org
Telecommunications Industry Assoc. **TIA**	Telecom Equipment	PBXs, Telephones, Cellular, PCS, Fiber Systems, Satellite, Radio Systems	TIA	Suite 300 2500 Wilson Blvd. Arlington, VA 22201 http://www.Tiaonline.org	Dan Bart 703-907-7703 703 907-7727 dbart@tia.eia.org
Society of Cable Telecommunications Engineers **SCTE**	Cable TV Systems, especially physical layer	Cable TV Components - cable, connectors, modulation	SCTE	140 Phillips Rd., Exton, PA 19341 http://www.scte.org/	Ted Woo 610 363-6888 610 363-5898

ATM Forum **ATMF**	ATM	User-Network Interface, Data Exchange Inte-rface,BISDN InterCarrier Interfaces, Private Network Node Interfca (PNNI)	ATMF	2570 West El Camino Real Suite 304 Mountain View, CA 94040 http://www.atmforum.com	Dawn Herman 415-949-6713 415-949-6705 info@ atmforum.com
Carrier Liaison Committee **CLC**	Telecom	Network Interconnection/Interoperability, Ordering and Billing, Industry Numbering, and Toll Fraud Prevention	Alliance for Telecommunications Industry Solutions (ATIS)	Suite 500 1200 G St. NW Washington, DC 20005 http://www.atis.org/	John Manning 202-434-8842 202-393-5453 jmanning@atis.org
National Committee for Information Technology Standards **NCITS**	Information Technology	Video, Imaging, Storage Media, Data Protocols	Information Technology Industry (ITI) Council	Suite 200 1250 I (Eye) Street NW Washington, DC 20005 http://www2.ncits.org/	202737-8888 202638-4922
Institute of Electrical and Electronics Engineers **IEEE**	Electrical and Electronics	Local Area Networks, Software Languages, Test and Measurements	IEEE	445 Hoes Lane Piscataway, NJ 08855 http://www.ieee.org/	Judy Gorman 908 562-3820 908 562-1571 j.gorman@ ieee.org
Internet Engineering Task Force **IETF**	Internet	TCP/IP and its Uses to Transport Information -Telnet, FTP	Center for National Research Initiatives (CNRI)	Reston, VA http://www.ietf.html	Steve Coya 703 620-8990 703 620-9913 scoya@ietf.cnri.reston.va.us

International Telecommunication Union - Telecommunications Sector **ITU-T**	Telecom	BISDN, SS7, IMT-2000, IN, TMN, SDH, Multi-media, Satellite, Fiber Systems, Radio systems, Broadcast Video	United Nations' ITU	U.S. State Dept 2201 C St NW Washington DC Geneva: ITU-T Place des Nations CH1211 Geneva 20 Switzerland http://www.itu.ch/	U.S. Earl Barbely 202 647-0197 202 647-7407 Geneva: Theo Irmer +41227305851
Network Management Forum **NMF**	Network Management	Service and Network Management	NMF	1201 Mt. Kemble Ave. Morristown, NJ 07960 http://www.nmf.org/	201-425-1900 201-425-1515
Satellite Broadcasting and Communications Association **SBCA**	Satellite Communications	Satellite Broadcast Equipment Earth Station Equipment	SBCA	Alexandria, VA http://www.sbca.com	703-549-6990
Satellite Industry Association **SIA**	Satellite Communications	Satellite Earth Station Equipment	SIA	225 Reinekers La., Suite 600 Alexandria, VA 22314 http://www.sia.org/	Clay Mowry 703-549-8697 fax 703-549-9188

9.4 PROCESS AND OVERSIGHT RECOMMENDATIONS FOR STANDARDS DEVELOPERS AND THE FCC

The information and recommendations contained in this section are provided specifically to aid in achieving the telecommunications interconnection objectives of Section 256 of the Telecommunications Act of 1996 ("TA96").

It is recognized that some standards developers to which the following recommendations apply have an international make up and that application of these recommendations by such organizations is specific to operations within the United States. Any application of these recommendations outside of the United States is taken to be solely a decision of and by the standards developer.

Definitions:

For this report, the term Standards Developer (SDs) is used to denote an organization that develops standards as defined in the Office of Management and Budget (OMB) Circular A-119 paragraphs “f” and “g.” In addition, paragraphs “d,” “g,” “i,” and “j” provide supporting definitions.

The OMB, in the revision to OMB Circular A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities,” has proposed that all Federal Agencies, including the FCC, use the following definitions:

f. **Standard** (or "technical standard," as found in P.L. 104-113), as used in this Circular, means: (1) common and repeated use of rules, conditions, guidelines or characteristics for products or related processes and production methods; (2) the definition of terms; classification of components; delineation of procedures; specification of dimensions, materials, performance, designs, or operations; measurement of quality and quantity in describing materials, products, systems, services, or practices; or descriptions of fit and measurements of size; (3) "performance standard" as defined above; or (4) "non-government standard," which is defined as a standardization document developed by a private sector association, organization or technical society which plans, develops, establishes or coordinates standards, specifications, handbooks, or related documents. The term does not include professional standards of personal conduct, institutional codes of ethics, or standards issued by individual companies. It also does not include standards created under other legal authority, such as those contained in the United States Pharmacopeia and the National Formulary, as referenced in 21 U.S.C. 351. A "Standard" may also be a "voluntary consensus standard," as defined below, or it may be what are commonly referred to as "industry standards" or "de facto standards," which are developed by industry associations which do not always adhere to the full consensus process.

g. **Technical Standard**, as used in this Circular, is synonymous with "standard." Examples of technical standards include, but are not limited to, size and strength specifications; technical performance criteria for a product, process, or material; test methods; procurement guidelines; sampling procedures; business practices; management systems; definitional standards; and installation safety codes.

i. **Voluntary consensus standards** are standards developed or used by voluntary consensus standards bodies, both domestic and international, and which are made available in a manner which includes provisions requiring that owners of relevant intellectual property have agreed to make that intellectual property available on a non-discriminatory, royalty-free or reasonable royalty basis to all interested parties. A "Voluntary consensus standard" may also be known in

common usage as a "voluntary standard," a "consensus standard," or a "consensus technical standard."

j. **Voluntary consensus standards bodies** are domestic or international organizations which plan, develop, establish, or coordinate voluntary standards using agreed-upon procedures. For purposes of this Circular, "voluntary, private sector, consensus standards bodies," as cited in P.L. 104-113, is an equivalent term. These bodies may include nonprofit organizations, industry associations, accredited standards developers, professional and technical societies, institutes, committees, task forces, or working groups. P.L. 104-113 and this Circular encourage the participation of government representatives in these bodies to increase the likelihood that the standards they develop will meet both public and private sector needs. A voluntary consensus standards body observes principles such as openness, balance of interest, and due process. Further, voluntary consensus standards bodies operate by consensus, which is defined as general agreement, characterized by the absence of sustained opposition to substantial issues by any important part of the concerned interests. Consensus requires that all views and objections be considered and that an effort be made toward their resolution.

9.4.1 Key Learnings

Examination of the history of post (Bell System) divestiture standards development by open private sector processes has shown it to be effective, with few exceptions, in the provision of technical standards required to support the interoperation and interconnection of the existing telecommunications environment. That history has also shown that the existing formal and information mechanisms for exchange of technical information and requirements between these processes and the Federal Communications Commission (FCC) are effective. Thus, it has been concluded that the current and evolving standards development processes are well positioned to meet the anticipated needs for technical specifications required to meet the objectives of Section 256 of TA96.

Past experiences with informal information sharing between the FCC and private sector standards developers has shown it to be an effective mechanism for coordination to meet governmental objectives via the development of voluntary public standards. These experiences have also shown that existing mechanisms for communicating FCC standardization requirements to the private sector processes have been effective.

The evolving and growing use of the Internet and the World Wide Web implementations have demonstrated the ever increasing value of the “Web” as a tool for information sharing among standards developers and between standards developers and other interested parties in the private and governmental sectors.

The American National Standard Institute (ANSI) Information Infrastructure Standards Panel (IISP) was established within the national voluntary standards system to accelerate development of standards critical to the Global Information Infrastructure (GII). An important characteristic of IISP is the cross-industry representation of its participants that includes the computer, communications, cable, broadcast, cellular and satellite industries. Representatives from

companies, government, standards and specifications developing organizations, architecture groups, industry associations and consortia are also involved.

IISP has over 70 actively participating organizations. The participant group comprises a broad spectrum of participants from the private and public sectors, with more than 30 standards organizations working with IISP to determine where existing standards meet requirements and where additional standards development efforts are required.

IISP has working groups in the areas of: Standards Framework Management, User/Content Provider Standards Requirements, International Aspects of the GII, and a Cross Industry Task Group. All of the groups are working toward identifying areas of standardization that may need to be developed in order to realize the full potential of the GII, and then collaborating with a broad range of standards and specifications developing organizations to determine if those needs can be met by existing standards and, where required, obtain agreement for development of needed standards for global use.

IISP has established a process for both identifying and reviewing standards needed to implement the GII. To date, IISP has identified over 130 Standards Needs in critical areas such as: interface requirements (*i.e.*: network to network, application to application, application to device, and network to device), security, electronic publishing, intelligent transportation and Nomadicity.

IISP working groups are continuing to identify standards needed in such areas as: device to device requirements, premises interface (business and residential), medical records, education, entertainment, electronic commerce, geographic information systems (GIS), knowledge management, and human factors.

After a need for a standard is identified, it is submitted for review within IISP, and it is also submitted to a group of organizations that have volunteered to review the standards needs identified by IISP. More than 30 standards and specifications developing organizations have volunteered to participate in the IISP Needs Review Process, and are presently reviewing the IISP Needs in order to identify any existing standards or standards projects that might fulfill the identified needs, and to determine where additional standards development efforts are required.

IISP recognizes that there may be standards or other publicly available specifications (existing or under development) that may meet the needs identified in whole or in part, and thus have sought the broadest possible participation of standards and specifications developing organizations so that costly duplication of effort is avoided. The feedback received from the standards and specifications developing organizations is an important part of the process. This iterative process is intended to help standards developers to agree on what still needs to be accomplished and how to do it in a way that keeps pace with technology being developed to meet user needs.

The standards needs identified by IISP, as well as the responses submitted, are entered into a database, which serves as a source of information on standards and the GII. The needs and responses are also circulated via IISP's WWW Home Page in order to get the broadest possible

review by all materially affected parties. Both Needs and responses can be submitted to IISP online via the web.

The Standards Roundtable is an IISP sponsored meeting with consortia and standards developers to review standards "Needs" (standard requirements identified by IISP) as well as to discuss existing standards and standards development programs that relate to those needs.

9.4.2 Recommendations

9.4.2.1 Recommendations to the Private Sector

Recommendation 1

When it is determined that a formal technical specification is needed to establish a telecommunications interconnection arrangement the following steps should be taken:

1. Conduct a search to determine if an existing standard will satisfy the technical need and apply it.

2. If the technical need can not be met by an existing standard, develop a high-level description and submit it to the (open and public) standards developer charged to develop the type of interconnect standard needed.

3. If either of the above two steps can not be performed due to a lack of knowledge about standards or the standards process, contact the American National Standard Institute (ANSI) Information Infrastructure Standards Panel (IISP) for advice.

CONTACT: Peter Lefkin Phone 212 642 4979
Internet: PLEFKIN@ansi.org

Implementation Target Date: Now

9.4.2.2 Recommendations to Standards Developers (SDs)

Recommendation 2

Standards developers should take steps to assure continuous improvement in their development and delivery processes. This should include the continued improvement and utilization of the Internet and the Web to advertise work programs, progress, and accomplishments.

Specific to the needs of Section 256, it is recommended that each standards developer establish a mechanism to support informal communications with the FCC to:

1. provide key tracking information on standardization activity related to the interconnection requirements of Section 256. The set of tracking information should include existing standards, standards under development and proposed work on new standards that may be related to the

FCC's *First Report and Order In the Matter of Implementation of the Local Competition Provisions in the Telecommunications Act of 1996 and Interconnection between Local Exchange Carriers and Commercial Mobile Radio Service Providers*, CC Docket Nos. 95-185 and 96-98 (August 8, 1996), Sections 212 and 366:

a) Six technically feasible interconnection points:
   (1) the line-side of a local switch;
   (2) the trunk-side of a local switch;
   (3) the trunk interconnection points for a tandem switch;
   (4) central office cross-connect points;
   (5) out-of-band signaling transfer points; and
   (6) the points of access to unbundled elements.

b) Seven unbundled network elements:
   (1) access to local loops;
   (2) network interface devices;
   (3) local and tandem switching capability;
   (4) interoffice transmission facilities;
   (5) signaling and call-related databases;
   (6) operations support systems functions; and
   (7) operator services and directory assistance facilities.

2. provide a documented process internal to the SD for review of concerns raised about standardization activities expressed by materially affected parties related to the goals of Section 256;

3. provide a duly appointed or elected FCC liaison officer to oversee related standards development activities related to Section 256 and other laws, and to provide a single point-of-contact on all related standardization issues.

Implementation Target Date: Year End 1997

9.4.3 Recommendations to Federal Communications Commission (FCC)

Recommendation 3

It is recommended that the FCC commit sufficient resources to provide:

1. a single point-of-contact for the informal exchange of information between the FCC and standards developers on activities related to the interconnection requirements of Section 256;

2. ongoing monitoring of standardization activities via the Internet and Web and, as required, through direct monitoring of key interconnection standardization activities at meetings.

Implementation Target Date: Year End 1997

Recommendation 4

The FCC may wish to continue an oversight role to address any issues that come before it on a complaint basis if some party believes that the standards process is not adequate to address their needs. In the first instance, the FCC should seek to have disputes resolved by manufacturers, service providers and/or end users; if they cannot resolve the issue, the FCC may need to get involved in the dispute.

Implementation Target Date: Now, and continuing

10. SPECIAL NEEDS OF CUSTOMERS WITH DISABILITIES

10.1 PROCEDURES OF STANDARDS DEVELOPMENT ORGANIZATIONS AND FCC PARTICIPATION TO PROMOTE TELECOMMUNICATIONS ACCESS TO INDIVIDUALS WITH DISABILITIES

Input was collected from members of Focus Group 2 and other sources. The input was discussed among the group and copies of the material and recommendations were circulated for comment to representatives of groups representing persons with specific disabilities.

10.1.1 Key Learnings

Persons with disabilities have unique requirements, depending on the nature of their disability, to use and access Customer Premises Equipment ("CPE"), network equipment, and telecommunications services. On the regulatory side, these accessibility issues have been addressed in a number of different forums. The FCC has conducted numerous rulemakings to address specific issues going back almost 20 years to CC Docket No. 78-50. Recent FCC activity has included rulemakings related to Hearing Aid Compatible ("HAC") telephones, Volume-Controlled telephones, Telecommunications Relay Services, Electromagnetic Interference ("EMI") concerns between wireless handsets and hearing aids, HAC requirements for wireless handsets, and an Inquiry (WT Docket No. 96-198) specifically addressing Section 255 of TA96, as well as the NRIC Charter to address access issues for persons with disabilities raised by Section 256 of TA96. The FCC has also established a special Disabilities Task Force and a web page to provide up-to-date information on these issues. (See http://www.fcc.gov)

In addition, Congress passed other legislation targeting the needs of persons with disabilities including the Americans with Disabilities Act ("ADA"), the Hearing Aid Compatibility Act, and other legislation covering issues such as closed captioning decoders and closed-captioned content requirements.

Other agencies of government are also involved in addressing many of these same telecommunications access issues and this includes the Architectural and Transportation Barriers Compliance Board ("Access Board"), the Department of Justice ("DOJ"), the Equal Employment Opportunity Commission ("EEOC"), the Department of Transportation ("DOT"), Health and Human Services ("HHS"), General Services Administration ("GSA"), U.S Postal Service ("USPS"), and the Department of Defense ("DOD"). Various agencies incorporate Access Board Guidelines in their rules.

The Access Board has generated several types of Guidelines documents addressing accessibility issues in the context of architectural, transportation, and communications barriers, and other federal agencies have adopted regulations incorporating some or all of these Access Board Guidelines. In addition, under Section 255 of TA96 the Access Board has established a Telecommunications Access Advisory Committee ("TAAC") comprised of representatives from industry, academia, and interest groups representing the needs of persons with disabilities to provide guideline recommendations to the Access Board for its use in an equipment accessibility rulemaking proceedings under Section 255. Information on TAAC and other telecommunications access issues can be found at http://trace.wisc.edu/world/tele_nav.html.

Various states also have state or local laws and regulations addressing the needs of persons with disabilities in the context of telecommunications and these local rules can cover Telecommunications Relay Services, access to operator services, volume-controlled coin telephones or credit card telephones, access to text telephones, and the provisioning of specialized CPE such as large button telephones, artificial larynxes, and other equipment used to provide greater access. (Also see Sections 64.606-64.608 of the FCC's Rules.)

In the voluntary, private sector standards area there are also many efforts to address the needs of persons with disabilities. There is an American National Standard, ANSI/CABO A117.1-1992, "Accessible and Usable Buildings and Facilities," which includes some telecommunications elements in its recommendations. This standard formed much of the baseline text for Access Board recommendations to implement the ADA, including the telecommunications portions of the ADA.

The American National Standards Institute ("ANSI") also sponsors the Information Infrastructure Standards Panel ("IISP") addressing the standards needs for National and Global Information Infrastructures ("NII/GII") and Working Group 4 of IISP addresses User Needs and has had presentations and discussions on the needs of persons with disabilities as a special class of user. The most recent needs presentation at IISP for persons with disabilities was given on November 13, 1996 by a Policy Analyst from the National Telecommunications and Information Administration ("NTIA"). Future IISP activities are also planned for 1997 in the area of needs of persons with disabilities. ANSI also has a Consumer Interest Council ("CIC") to reflect all consumer issues in the voluntary standards process and to provide linkage to international standards groups which have activities targeted to consumer needs such as the International Organization for Standardization's ("ISO") Consumer Policy Committee ("COPOLCO"). The needs of persons with disabilities can be accommodated with the appropriate participation by representatives of these interest groups in the voluntary standards process, especially on the ANSI CIC, ANSI IISP, and directly with specific SDs.

ANSI-accredited standards development organizations also have programs in their technical competency areas directed to satisfying standards needs for equipment or services to provide improved accessibility to communications for persons with disabilities. For example, the Telecommunications Industry Association ("TIA") produced the standard that is used by the FCC to determine HAC compliance for corded and cordless and Integrated Services Digital Network

("ISDN") telephones in Part 68 of the FCC's rules. (See 47 C.F.R. Section 68.316) TIA also had a project attempting to create a standard for Text Telephones or devices often called Telecommunications Devices for the Deaf ("TDDs") or TTY devices. More recently, TIA's Engineering Committee TR-30 worked very closely with the International Telecommunication Union ("ITU") to produce ITU Recommendation V.18, "Operational and interworking requirements for DCEs operating in the text telephone mode." This international standard provides technical requirement for Text Telephone compatibility.

TIA and the Institute for Electrical and Electronics Engineers ("IEEE") standards were also used by the FCC in its Order in CC Docket No. 87-124 to specify volume control requirements for new telephones. TIA was also active in the FCC's Negotiated Rulemaking Committee addressing Hearing Aid Compatibility ("HACNRC") and a TIA Director is the present Chair of the TAAC. Since technical needs of persons with disabilities do not have geo-political boundaries, liaison by ANSI accredited SDs with other SDs worldwide provides additional input for the voluntary standards process. For example, TIA and Committee T1 have close relations with the European Telecommunications Standards Institute ("ETSI") and thus have access to standards projects and draft standards being generated in Europe that may address standards needs of persons with disabilities. Similarly, TIA and Committee T1 work closely with the Canadian Standards Association ("CSA") and would have similar input and access to standards work from our Canadian colleagues.

Under Chapter 13 of the North American Free Trade Agreement ("NAFTA"), the U.S., Canada and Mexico included "access" to public telecommunications transport networks and services as one of the treaty provisions at Section 1304-1(e). TIA, as the USA Secretariat to the Consultative Committee on Telecommunications ("CCT"), has been advised that this term refers to access by persons with disabilities and includes, for example, the Hearing Aid Compatibility Rules of the FCC. Thus, if the Commission, by rules implementing Section 255, were to expand the scope of access under NAFTA, close cooperation with Canada and Mexico would be required. And the scope of required coordination among governments promises to increase under initiatives such as the Free Trade Agreement of the Americas. Voluntary standards groups such as TIA and Committee T1 work with all of their colleagues in this hemisphere and globally to attempt to harmonize specific standards.

The Electronic Industries Association ("EIA"), another ANSI-accredited SD, is also actively concerned with the needs of persons with disabilities. The EIA Consumer Electronics Manufacturers Association ("EIA CEMA") has an Assistive Devices Division and EIA standards are used for closed captioning in television sets. The Electronic Industries Foundation ("EIF"), in cooperation with the CEMA Assistive Devices Division has also produced a guidelines document for accessible design of consumer electronics products. EIF has conducted considerable outreach to various groups representing persons with disabilities to get their perspectives on the work of EIF. Drafts of the EIF Guidelines document have been presented at TAAC, and EIA CEMA is represented in the TAAC.

10.1.2 Recommendations

Recommendation 1

Focus Group 2 believes the current procedures in place at ANSI, IISP, TIA, EIA, Committee T1, and other SDs, both domestically and internationally, are adequate to capture standards needs and provide input to the standards process when these procedures are utilized by groups representing persons with disabilities. More active participation by groups representing persons with disabilities in the standards process is encouraged including submission of contributions and comments on the draft standards when they go through the public review period. Such groups should also become active in the ANSI Consumer Interest Council.

Implementation Target Date: Now

Recommendation 2

SDs should include a step in the establishment of new work that draws attention to the needs of individuals with disabilities.

Implementation Target Date: 1Q98

Recommendation 3

SDs should notify the FCC of any new standardization work that may uniquely impact individuals with disabilities.

Implementation Target Date: 1Q98

There are numerous outreach mechanisms currently in place including ANSI CIC, IISP, COPOLCO, TAAC, CEMA Assistive Devices Division, EIF, and SD standards activities. In addition, these same parties are active in regulatory proceedings before the Access Board and the FCC addressing the needs of persons with disabilities. Other industry groups such as the Cellular Telecommunications Industry Association ("CTIA"), Personal Communications Industry Association ("PCIA"), United States Telephone Association ("USTA"), and Alliance for Telecommunications Industry Solutions ("ATIS") have worked with representatives of the disability community on mutual topics of interest for addressing the needs of persons with disabilities. This includes participation in programs and conferences from such groups and organizations as the World Institute on Disabilities, the Association for Safe and Accessible Products, TEDI, the National Center for the Law and Deaf ("NCLD"), the National Office on Disabilities ("NOD"), and the Paralyzed Veterans Association ("PVA"), among others.

Recommendation 4

The FCC should encourage the existing outreach programs to continue and join with industry in sponsoring human resource training programs that provide guidance to equipment designers about the wide range of accessibility needs of persons with disabilities. As new technologies become available to facilitate accessibility the FCC should monitor such developments and provide public notice of such innovations.

Implementation Target Date: Now, and continuing

Recommendation 5

On the regulatory side, the FCC will need to conclude its Inquiry under Section 255 and take whatever actions it deems appropriate under Section 256. The cooperative activities of the Telecommunications Access Advisory Committee ("TAAC") have demonstrated how industry and consumer groups can work together to solve accessibility problems and achieve a high degree of consensus. The Commission should work closely with the Access Board as it develops its Guidelines and provide the FCC's guidance and recommendations from the record created in response to the FCC's Inquiry in WT Docket No. 96-198.

Implementation Target Date: February - August 1997 as Access Board develops Guidelines.

Recommendation 6

On the voluntary standards side, Focus Group 2 recommends that the FCC follow the recent guidance given by Congress to all federal agencies in the National Technology Transfer and Advancement Act of 1996 ("NTTAA"). In addition it recommends that the FCC utilize voluntary standards for regulatory purposes and participate directly in the standards creating process. Specifically, Section 12 of the NTTAA states:

Section 12 . . .
(d) UTILIZATION OF CONSENSUS TECHNICAL STANDARDS BY FEDERAL AGENCIES; REPORTS-
(1) IN GENERAL- Except as provided in paragraph (3) of this subsection, all Federal agencies and departments shall use technical standards that are developed or adopted by voluntary consensus standards bodies, using such technical standards as a means to carry out policy objectives or activities determined by the agencies and departments.
(2) CONSULTATION; PARTICIPATION- In carrying out paragraph (1) of this subsection, Federal agencies and departments shall consult with voluntary, private sector, consensus standards bodies and shall, when such participation is in the public interest and is compatible with agency and departmental missions, authorities, priorities, and budget resources, participate with such bodies in the development of technical standards.
(3) EXCEPTION- If compliance with paragraph (1) of this subsection is inconsistent with applicable law or otherwise impractical, a Federal agency or department may elect to use technical standards that are not developed or adopted by voluntary consensus standards bodies if the head of each such agency or department transmits to the Office of Management and Budget an explanation of the reasons for using such standards. Each year, beginning with fiscal year 1997, the Office of Management and Budget shall transmit to Congress and its committees a report summarizing all explanations received in the preceding year under this paragraph.
(4) DEFINITION OF TECHNICAL STANDARDS- As used in this subsection, the term `technical standards' means performance-based or design-specific technical specifications and related management systems practices.

Recommendation 7

By direct participation in the standards process, where appropriate, the FCC can bring its wisdom and insights directly to the SDs. At a minimum, the FCC may wish to

reserve an oversight role to address any issues that come before it on a complaint basis if some party believes that standards being generated are not adequate to address its needs. In the first instance, the FCC should seek to have disputes resolved by manufacturers and service providers and only involve the FCC in the event the matter can not be resolved. This approach would also be in keeping with other Congressional guidance in another area, where in the Communications Assistance for Law Enforcement Act of 1994, Congress again deferred to the voluntary, consensus standards process, and limited the FCC's role to one of oversight if some party believed the resultant industry standard was in some manner deficient.

Implementation Target Date: Now

11. INFORMATION SERVICES FOR RURAL CUSTOMERS

11.1 PROCEDURES OF STANDARDS DEVELOPMENT ORGANIZATIONS AND FCC PARTICIPATION TO PROMOTE TELECOMMUNICATIONS ACCESS TO INFORMATION SERVICES IN RURAL AREAS

As used herein, per the Telecommunications Act of 1996, an "INFORMATION SERVICE" is the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.

As used herein, again per the Telecommunications Act of 1996, a "RURAL TELEPHONE COMPANY" is a local exchange carrier operating entity to the extent that such entity-
(A) provides common carrier service to any local exchange carrier study area that does not include either-
(i) any incorporated place of 10,000 inhabitants or more, or any part thereof, based on the most recently available population statistics of the Bureau of the Census; or
(ii) any territory, incorporated or unincorporated, included in an urbanized area, as defined by the Bureau of the Census as of August 10, 1993;
(B) provides telephone exchange service, including exchange access, to fewer than 50,000 access lines;
(C) provides telephone exchange service to any local exchange carrier study area with fewer than 100,000 access lines; or
(D) has less than 15 percent of its access lines in communities of more than 50,000 on the date of enactment of the Telecommunications Act of 1996.

11.1.1 Key Learnings

Rural telephone companies can learn about standards that are being developed through membership in the Organization for the Promotion and Advancement of Small Telecommunications Companies (OPASTCO). OPASTCO educates their membership and collects information from their membership by member involvement in the OPASTCO Technical Committee and the OPASTCO Standards Forum. The OPASTCO members are able to identify standards activities they need to participate in through involvement in the two committees.

One way for rural telephone companies to participate in the standards development process is through membership in the United States Telephone Association (USTA). USTA collects information on rural needs through member involvement in the Technical Discipline committees and through surveys of the membership. Then, the staff of USTA represents the membership at Standards Forums. USTA is represented in all of the Committee T1 Committees and in many of the consensus forum activities which are continuing to increase in importance because many agreements need to be reached as part of the input to standards development.

USTA participates in the Alliance for Telecommunications Industry Solutions (ATIS) sponsored Carrier Liaison Committee (CLC), the Ordering and Billing Forum (OBF), the Network Interconnection Interoperability Forum (NIIF), the Industry Numbering Committee (INC), the Toll Fraud Prevention Committee (TFPC), and other consensus forums.

Additionally, rural telephone companies may also directly participate in any ATIS sponsored forum, as they are all open to interested and materially affected parties.

11.1.2 Recommendations to the Federal Communications Commission (FCC*)*

The following actions by the FCC are recommended to promote access to information services by subscribers of rural telephone companies:

Recommendation 1

The FCC and the rural telephone industry should work together to educate all telecommunications providers about where and how different types of standards are developed. The FCC and the industry should jointly sponsor a seminar(s) explaining how rural carriers can participate in standards development.

Implementation Target Date: *To be determined*

Recommendation 2

The FCC is encouraged to monitor the standards process so they remain informed about the activities taking place in the standards forums.

Implementation Target Date: Now, and continuing

Recommendation 3

The FCC should encourage all standards bodies to allow telecommunications providers to access information regarding developing standards and provide input to standards via telecommunications.

Implementation Target Date: Now, and continuing

Recommendation 4

The FCC may wish to continue an oversight role to address any issues that come before it on a complaint basis if some party believes that the standards process is not

adequate to address their needs. In the first instance, the FCC should seek to have disputes resolved by manufacturers, service providers and/or end users; if they cannot resolve the issue, the FCC may need to get involved in the dispute.

Implementation Target Date: Now, and continuing

12. ABSTRACT OF ALL NRIC RECOMMENDATIONS

The number preceding each recommendation below corresponds to the number of the section in the focus group report in which that recommendation appears. Numbers in brackets have sometimes been added where more than one discrete recommendation appears within a section. The recommendations below have sometimes been slightly abridged, with elisions and explanatory additions according to the usual conventions for quoted material.

4.1.2.1
The planning of network architectures, including *Architecture Definitions (Goals / Objectives / Concepts)*, *Standards Developers*, and *Requirements Documentation* as shown on the Services Planning Process Model (Figure 1), should be performed by a field of industry participants that includes, but is not limited to, Service Providers or their representatives, Equipment Suppliers, Regulatory Bodies, Industry Consultants, Users, Interest Groups, and anyone with a vested interest in telecommunications products or services. Additionally, since the ability to comply with network reliability obligations and interconnectivity requirements, and offer nondiscriminatory accessibility hinges on such participation, it should be encouraged.

4.1.2.2
"Open Forum" activities are associated with the concepts of joint planning and information sharing and should be worked in a manner that is unrestricted and accessible to all interested participants. The activities shown on the Services Planning Process Model (SSPM) (Figure 1) for National Services including *Service Requirements / Documentation, Architectures Goals / Objectives / Concepts*, *Standards Developers*, and *Requirements Documentation* shall be considered "Open Forum" activities.

4.1.2.3
Specific activities in the planning of network architectures should be performed by the participants (see 4.1.2.1) and are considered "Open Forum" activities (see 4.1.2.2). The following list… is not all inclusive but is representative…:

- Selection of applicable technologies
- Identification of functional requirements of technologies
- Identification of points of open connection (see Section 9.4.2.2)
- Selection of technical standards for open interfaces
- Development of interoperability testing requirements
- Identification of applicable network support system requirements
- Identification of operational impacts

4.1.2.4
Specific activities in the planning of network implementations should be performed by the Service Providers and their Vendor(s) and shall be considered "Closed Forum" activities (see 4.1.2.2). The following list of activities is not all inclusive but is representative of the focus on the "When?", "Where?", and "How-much?" for Planning Network Implementations:

- Equipment identification and deployment areas
- Equipment interconnection specifics
- Network dimensioning (e.g., traffic engineering, capacity planning, *etc.*)
- Service option selection by Market Area
- Vendor product selection
- Economic evaluation of deployment alternatives
- Identification of budgetary requirements
- Vendor contract negotiations and placements
- Determine engineering criteria
- Develop and implement new or changed operating procedures
- Develop equipment forecasts
- Negotiate standard provisioning intervals

4.2.2.1
The process for National Services planning should begin with the development of a service definition which provides the feature characteristics of the service. Included in the definition are details on the geographic scope as well as service provider scope of the service. It also includes backwards compatibility requirements and the extent of interconnection and interoperability required for the service. As to level of detail, the service definition needs to be sufficiently specific to provide a planning basis that identifies all of the characteristics that must be achieved in practice as a result of completion of the implementation process.

4.2.2.2
The planning for National Services, like the planning for Network Architectures (see 4.1.2.1), specifically *Service Requirements / Definitions* as shown on the Services Planning Process Model (Figure 1), should be performed by a field of industry participants that includes, but is not limited to, Service Providers or their representatives, Equipment Suppliers, Regulatory Bodies, Industry Consultants, Users, Interest Groups, and anyone with a vested interest in telecommunications products or services. Additionally, since the ability to comply with network reliability obligations and interconnectivity requirements, and offer nondiscriminatory accessibility hinges on such participation, it should be encouraged.

The proposed new environment presented in the Telecommunications Act of 1996, in regard to National Services planning, must fairly take into account all of the issues involved in the deployment of services on a widespread basis. Provisions must be made for functions known to be required such as specification development, trials and testing, and large scale interoperability testing when necessary. Effects of new services on support systems and the requirement that new

network functions and services must not compromise the utility of existing services or network reliability must be established.

National Services planning should make use of the currently available structural resources of the telecommunications industry and develop one additional function that would provide an overall coordination capability for the management of both planning and coordination activities. This new function should have the following characteristics:

- The National Services planning and coordination function should be organized as part of the industry consensus process. It should accomplish many of the functions of a federal advisory committee, but should not be formally impaneled as such.

- Each National Service should have its own dedicated planning and coordination activity, managed by a service-specific group.

- A specific group of industry experts should be assigned by industry entities to populate each service-specific planning and coordination function.

- The planning and coordination function should serve as a voluntary industry management resource, acting on behalf of the industry and its regulators.

- Each group will utilize resources in the industry necessary to complete all of the work activities necessary to accomplish successful service introduction.

- The management activities can be disbanded upon successful service introduction continued in a maintenance mode. National Services must be maintained as such.

4.2.2.3
National Services planning and Network Architectural planning activities need to be closely coordinated and interactive. Early in the planning process, the necessary architectural resources must be identified. From that, assessments can be made as to the utility of existing architectural assets, in order that effective and timely planning may begin early for enhancements to existing resources or additional resources identified as may be required.

4.2.2.4
Both processes that make up the SPPM, the Planning for National Services and the Planning for Proprietary / Regional Services, need to provide information to and feedback from all service providers that are affected on order that they may accomplish the necessary activities and acquisitions in their portions of the network on a known and reasonable schedule.

4.2.2.5

The FCC should oversee the planning of National Services as recommended in Section 4.7.2 of this report. For the planning of Proprietary / Regional Services, the process will continue to be outside of the Commission's oversight until and unless, formal action occurs to change such services to National Services, with the obvious exception that any Proprietary / Regional Service structure cannot interfere with or defeat the intent of any service that is national in scope. In such cases, the Commission could well take action as necessary to prevent interference, but would still not play an affirmative role in planning the elements of a sub-national service.

4.3.2.1
Since market forces will continue to be a key determinate of how and when architectures, products, and services are developed and deployed, proprietary implementations will persist. Therefore, the National Services Planning process needs to address the transition of Proprietary / Regional Services and products to a public status…. [Service requirements] should be flexible enough to handle the many transition possibilities and contain industry accepted criteria to promote the expeditious development of the interconnection and interoperability requirements for National Services.

4.4.2.1
For National Services and Products, a new Forum should be established as per *Recommendation 4.2.2.2 Participation* and *Activities in Planning for National Services*. Moreover, ATIS, or other telecommunications industry committees or organizations, should develop a proposal, for industry review, for the establishment and management of such a forum.

4.4.2.2
Network Architecture planning activities as described in *Recommendation 4.1.2.3 Activities Considered Part of Planning Network Architectures,* should be pursued with the newly formed Network Interconnectivity / Architecture (NIA) Committee. To accomplish this, the chair of the NIA should develop a proposal, for industry review, to add the management of Network Architecture Planning activities as an additional functional area to their Committee's responsibility.

Additionally, because of the required close working relationship between both a National Services and Products Forum and a Network Architecture Planning Activities Forum, if the outcome results in two separate forums, there should be a requirement in place that they be managed under a common "umbrella" organization to insure the requisite integration of the individual activities is accomplished.

4.5.2.1
The position of service providers and vendors to protect competitively sensitive information will continue to be appropriate when dealing with products and services that have not been mandated by the federal government for national availability…. The telecommunications industry should have the freedom to develop innovative products and services so their business can thrive and grow in the telecommunications marketplace.

4.5.2.2

As shown on the Services Planning Process Model (Figure 1), the interaction and sharing of information between telecommunications Service Providers, Vendors, Users, Interest Groups and Regulatory Agencies is necessary for the efficient development of National Services (Mandated or Voluntary) (see 4.2.2.2). The *Requirements Documentation* activity of the SPPM for National Services will specify, along with a number of other outputs, the appropriate interface requirements for the product or service providing each telecommunications service provider and vendor the means to understand the interoperability issues involved. Telecommunication vendors are then able to develop proprietary technical specifications that are required for their equipment. Such vendor-specific implementations may be considered proprietary but can still be capable of meeting interoperability and interconnectivity requirements if there is strict adherence to the national specifications and requirements.

4.6.2.1
Based on the process flow on the Services Planning Process Model (Figure 1) for National Services (Mandated or Voluntary), architectures, services, and features will be implemented as "standard", not proprietary. The "Open Forum" activities (see 4.1.2.2), including *Standards Developers*, are designed to lessen the impact of a lengthy time interval in producing a requirement, through cooperation and sharing by the industry participants in the process (see 4.2.2.2) and still meet interoperability and interconnectivity requirements.

4.7.2.1
The federal government should not be directly involved in the internal development of technical specifications by telecommunications service providers and vendors. Neither should it be directly involved in the development of Proprietary / Regional Services that are not considered national in scope (see 4.2.2.5).

4.7.2.2
The role of the federal government in monitoring network planning in the telecommunications industry should be that of oversight. The FCC should monitor telecommunications Standards Forums (Accredited & Consensus) activities, as recommended by Focus Group 2, to ensure that interoperability is maintained as a goal during the development of National Services and/or Products. This can be accomplished by advising the FCC of the industry forum activities during the early stages of National Services definition.

4.7.2.3
The FCC should work cooperatively with the industry processes (e.g., consensus forums, standards bodies, *etc.*) in order to accomplish key interoperability and reliability objectives. The FCC should respond to industry forum requests for action (issue resolution) that emanate from either the *Service Requirements/Definitions* or the *Architectures Goals/Objectives/Concepts* activities of the National Services Planning process and are specific to Section 256 of the Telecommunications Act of 1996, using the most expeditious mechanism available to respond to the industry's needs. A process should be created to allow the industry to escalate such issues directly to the FCC for resolution. The Commission need not take any action, other than their oversight role, unless requested to do so, using the escalation process, by one or more of the industry forums.

5.1.2
Due to the Telecommunications Act of 1996…, the various industry segments should organize themselves to ensure that risks to interoperability are minimized through such means as increased information sharing and improved liaison processes.

5.2.2.1
Because of the breadth and scope of the NRC II compendium, the templates may not have found their way to the personnel involved in current interconnection agreement negotiations. After an initial review of the templates, the Implementation Task Group felt that an immediate re-dissemination of the original templates was timely as many companies were already engaged in negotiations (**no additional action necessary**).

5.2.2.2
The Implementation Task Group reviewed [enhanced and modified] the templates in light of the experience gained by participants in local interconnection negotiations as well as in the implementation of the Telecommunications Act of 1996. Most of the changes to the Network Interconnection Bilateral Agreement Template reflect the reorganization of sections based on functionality, the clarification of the purpose of these sections, and the addition of relevant topics to these sections (**no additional action necessary**).

5.2.2.3
The Implementation Task Group recommends… disseminat[ation of] the revised Network Interconnection Bilateral Agreement Template under separate cover to those working level personnel targeted for the NRC II template(s) re-distribution effort [by the NIIF]

5.2.2.4
Depending upon the wishes of the negotiating parties, the Bilateral Template may be used either as one complete unit or as a means to address particular issues individually. For example, addressing issues individually may ensure that key points regarding that issue are not overlooked. Examples of these types of issues include network interconnection, unbundling, and resale. This method may be helpful as perspectives may change depending upon the issue under consideration. Furthermore, in order for the Bilateral Template to remain a viable tool, future revisions may be necessary. As other emerging issues become more well defined, future additions and revisions will be required.

5.2.2.5
The recommended custodian of the Bilateral Template is the Network Interconnection and Interoperability Forum (NIIF), sponsored by ATIS…. The NIIF is recommended to regularly review the Network Interconnection Bilateral Agreement Template and amend it as necessary. The Implementation Task Group further recommends that the NIIF establish processes (or use existing processes) to facilitate the review and update of this template. These processes should include, at a minimum, that template users, whether or not they are NIIF participants, are able to submit suggestions for changes/additions by contacting the NIIF Director resident at ATIS. The

importance of having user-friendly processes to update the Network Interconnection Bilateral Agreement Template is emphasized.

5.3.1.1
In order to centralize sources of available information, the Task Group recommends the establishment of a homepage as a billboard and as a single source for activities and issues related to the implementation of interconnection. Such a site could also then serve as the catalyst for liaisons. If users of the site find valuable information on an important interconnection issue to their company, they will have information on how to contact the organization, group or company that worked on the matter, and could establish a liaison to find more information.

5.3.1.2
The Task Force further recommends that the NIIF create and maintain the site. It is recognized that the NIIF has its own site on the ATIS homepage and could fulfill this recommendation by establishing a single source as part of its existing site. The Task Group contemplated that the NIIF would establish the necessary liaisons with other organizations and industry groups both inside and outside of the ATIS ranks, to gather information on those industry efforts addressing interconnection and interoperability. The NIIF could then post this information on its website. The goal of this exercise is to establish a central repository for this kind of information. In some cases, this exercise may include a mere notice as to certain work ongoing in another organization. In other instances, it may include actual procedures developed by an industry group on how to address a specific issue.… It was also contemplated that ATIS and NIIF do what is necessary to publicize the existence of this site.

5.3.2.1 The NIIF should be directed to take a broader responsibility for the template, including the establishment of liaisons with other industry committees, forums, and organizations whose expertise would help maintain and expand the template as needed and as appropriate. Such candidates for NIIF liaisons are the Ordering and Billing Forum (“OBF”) for those elements of the template which may have billing system impacts for service providers. Another example would be a liaison with Committee T1 on the national standards developed for interconnection or even a liaison with the National Cable Television Association to learn if any work in that organization would impact the templates and thus, warrant amending the templates. If there were no direct impact to the template, but information was provided by the cable industry on how they addressed an interconnection issue, it might be worth sharing via the homepage as discussed above. Where there are other groups which have responsibility for the matters within the template, the Task Force recommends that the NIIF seek out the appropriate liaisons with other industry groups as part of its responsibility for the template.

5.3.2.2
In addition to the immediate dissemination of the template as recommended in Section 5.2.2, it is important that the template be made available on a regular basis, particularly as changes are made. The Task Group recommends, at a minimum, that it be posted on the NIIF homepage. The Task Group suggests that other forms of dissemination should be considered by the NIIF. This activity will begin to centralize this important information.

5.4.2.1
A few additions could be made to the sources of information to which the FCC's homepage provides links. For example, there does not seem to be a direct link from the Mackie-Mason site to the homepages of the various state PUCs, and some important trade associations are missing.

The Implementation Task Group encourages the FCC and these organizations work jointly to ensure that listings are posted on the FCC website(s).

5.4.2.2
Currently the FCC maintains a Consumer Resources area on the Common Carrier Bureau website. This area has customer satisfaction reports, frequently asked questions, and access to other telecommunications sites. A similar area for telecommunications providers should be created. This area could use the same access to other telecommunications sites as the Consumer Resources Area does. It could have its own frequently asked questions. If appropriate, customer satisfaction reports on suppliers to telecommunications providers could also be made available.

5.4.2.3
The Task Group suggests that trade associations develop primers on interconnection and interoperability issues as part of the educational programs that they provide for their membership. The NRIC report could serve as initial input into this process.

6.1.1
The FCC Order in Docket 96-98, Paragraph 523, states "We thus conclude that an incumbent LEC must provide nondiscriminatory access to their operations support systems functions for pre-ordering, ordering, provisioning, maintenance and repair, and billing available to the LEC itself. Such nondiscriminatory access necessarily includes access to the functionality of any internal Gateway systems."

- To facilitate meeting the FCC Order's functionality requirements, the Gateway will be subdivided into components and subsystems based upon business functions, interfaces, auditing functions and security.
- Though it may appear to be a single Gateway per access type to the individual CLEC, separate Gateways may be built to provide the required functionality to support the five business functions (pre-ordering, ordering, provisioning, maintenance & repair, and billing). This allows the architecture of the Gateway to have modular components. Based upon this concept, flows between the individual components of the overall system can be identified and designed.
- The Gateway will be able to translate to a commonly agreed upon standard format (LSR standardized formats or EDI formats). These formats will be mutually agreed to and will be the basis of requests submitted to the Gateway to be communicated to the ILEC legacy OSS.
- The Gateway function represents a set of mediation services between an ILEC and the CLECs which provides for the exchange of data in agreed-to standard formats. EDI and the proposed LSR are potential candidates for this format. Because of its long history, EDI may be more prevalent for the pre-ordering, ordering, provisioning and billing business functions while a mix of EDI and managed object-based formats compliant with TMN and

International Standardization Organization (ISO) standards will be used for the maintenance and repair functions.

- Whenever and wherever possible, data collected from one transaction through the Gateway should be available to populate a subsequent transaction through the Gateway, *i.e.*, data collected from a pre-ordering transaction will be used to populate an ordering transaction. The data should be buffered and populated by the CLEC originating the transactions.

6.1.1.2

The electronic Gateway interface should be developed using the most currently accepted computing architecture design standards in order to provide equal access for all CLECs. It should be recognized that once the Gateway is implemented and operational, any lack of availability of the Gateway will be service impacting to the users.

Since multiple CLECs will most likely use multiple computing environments that may or may not be similar to the ILEC's computing environment, the Gateway should be developed in a manner that will permit all CLECs to attach to the Gateway using an efficient method. This Gateway should also be developed in such a manner that it is maintainable in a technically secure environment.

The electronic Gateway should be accessible through at least four network access subsystems. These are private line, dial-up, EDI, and Internet based access as appropriate for the various types of functionality. While it is recognized that OSI interfaces are at the core of telecommunications standards, it is recommended that use of the Transmission Control Protocol/Internet Protocol (TCP/IP) family be used for access to facilitate encompassing as wide a potential CLEC audience as possible.

- Private Line interfaces: Private line interfaces will be made available. This technology will be firewalled in such a way that the ILEC's and the CLEC's data are protected from one another. Where applicable, local address mapping may be applied to facilitate routing data to the electronic Gateway of the ILEC. Routing protocols used for this type of interface will be based upon Internet Engineering Task Force (IETF) standards with Open Shortest Path First (OSPF) or Border Gateway Protocol (BGP) preferred.
- Dial-up Access: Access to the Gateway will be made available by means of dial-up access. In-dials will be secured using the IETF proposed standard RADIUS methodology or secure ID Card technology. A variety of options relating to speed and technology will be afforded. ISDN access will be recommended because of its speed and versatility. Point to Point Protocol (PPPs) will be used over these linkages.
- Internet interfaces: Access to the Gateway will be available using the Internet. Access to the Gateway will be provided by means of a web interface. This technology will be firewalled in such a way that the ILEC's and the CLEC's data are secured from one another.
- EDI interfaces: Access to the Gateway is normally through a Value Added Network (VAN) using, as an example, X.25 protocol or dial-up. These interfaces are available through a variety of service providers.

The Gateway should provide continuous availability using High Availability technology with processor failover in the event of a processor failure or fully redundant subcomponent structure. Generally, failure of a module should trigger the initiation of a redundant processor to allow the system components to continue to operate. In addition, it is expected that these systems should reside in a 24-hour per day, 7-days a week (24x7) facility and should have battery backup and standby power systems. The computing architecture will support replacement of components without requiring the operator to power down the Gateway. System predictive monitors for failing components and multiple fault-tolerant processors are recommended in the Gateway design. Multithreaded operating systems are recommended where possible to ensure highest performance in processing transactions. The computing architecture of the Gateway should be scaleable to allow for growth traffic and functionality.

6.1.1.3

Without some Congestion Control process in place, it is conceivable that a CLEC, either intentionally or unintentionally, could prevent other CLECs from accessing the Gateway. The ILEC should be responsible for ensuring that all CLECs have an equal opportunity to access the Gateway. The ILEC should also be responsible for monitoring the traffic across the Gateway in order to manage it and to maintain predetermined standards for flow-through.

- Ensure that each CLEC is afforded a choice of network access methods to the electronic Gateway.
- A software tool should exist to detect congestion problems within individual components of the Gateway(s).
- A software tool should exist to isolate problems affecting the Gateway and facilitate clearing the problem. This should be developed using TMN standards and other international standard technology.
- Provide a subsystem to document congestion in each access mechanization and report malicious activities to the FCC or appropriate authorities. Standards based network management tools, using Common Management Information Protocol (CMIP)/Common Management Information Services Element (CMISE) and Simple Network Management Protocol (SNMP), will be applied.
- A software tool should be provided to monitor telemetry and performance data in the Gateway and between distributed systems that the Gateway relies upon.
- Traffic and capacity of Gateway and access links will be modeled to identify probable bottlenecks and suggested data points.
- A traffic engineering module should be developed to determine blocking factors provided by current network access methods of the Gateway.
- A non-discriminatory access or queuing algorithm should be developed to accommodate unusual traffic patterns so that each CLEC has an equal probability of obtaining access into the Gateway during these events.
- Reporting software tools should be developed to document response time, congestion and Gateway usage for each CLEC.

- Software tools should be provided to document mean-times to resolution for alarms, for fulfillment of specific business function requests, and for comparisons of response times between an ILEC and a CLEC and between a CLEC and another CLEC.
- Insure that no single or group of CLECs is favored over any other CLEC or group of CLECs.

6.1.1.4

As competing companies increasingly share systems and data, access to those resources must be secured. Without a full range of security measures in place, both systems and data are in danger of misuse, corruption, and loss of confidentiality.

Before any access security methods can be effected, agreement must be reached as to the kinds of data that will be shared. Customer confidentiality and proprietary data must be protected while common data must be readily available to all authorized users. It is recommended that the classification of the data be resolved by the CLECs and ILECs as quickly as possible.

There are many ways companies may share information including LAN-to-LAN connections, VAN connections, dial-in connections, and public Internet access. The degree to which each of these must be secured varies. Key facets to secured transactions are identification, authentication, access control, data integrity, data confidentiality and non-repudiation. It is recommended that Access Security reach the High Level of Security Requirements contained within ANSI T1, 233, 243, and ITU-T.

- **Encryption** will be central to several aspects of security. It can serve as safeguard against unauthorized recipients interpreting transmissions, thereby protecting confidentiality and preventing fraud. It can limit damage caused by an individual or system entering a command, intentionally or otherwise, that destroys a file system. Encryption can provide authentication of the message originator and the system user. Electronic certification and digital signatures can protect against unauthorized modification and forgery of documents. No encryption is recommended for LAN-to-LAN or VAN communications so long as the LAN, VAN or environments in between are reasonably secured to industry standards such as the ANSI T1 233, Bellcore *Generic Requirements For Data Communication Networks*, TR-STS-0001332, *etc.*. For dial-up or Internet access, a more sophisticated process algorithm will be a necessity. Secure Socket Layer (SSL), Secure Multipurpose Internet Mail Extensions (S/MIME), secure IP tunneling, and X.509 are examples of accepted methods for providing confidential exchanges on the Internet; an equivalent solution is recommended for dial-up. While these methods may affect the throughput of transactions, anything less is subject to interception and interpretation by unauthorized parties. It is further recommended that vendor-proprietary algorithms should be avoided because they frequently have not been subjected to a thorough industry-wide analysis.

- **Authentication** involves establishing a proof of identity. With any connection, some form of ID/password is crucial. With dial-in and public Internet access, the use of one time passwords, a security calculator or "smart card" is recommended. Further, encryption of the

user identification and password is critical when data is transmitted over the public network via dial-in or public network access.

- **The trusted third party concept** is essential to authentication. With a trusted third party, neither the user nor the host relies solely on the credentials supplied by the other.

- **Access control and data partitioning** relates to whom or what may have access to data and resources to protect competitive information, data, and systems. Since identity is at the core of access control, its implementation requires some form of authentication.… While the access control policies should be constant across all access methods, implementation may vary.

- Filtering must be done on both incoming requests and their responses.… Other filtering will be required for each message response.

- For data field security and record level security, it is recommended that a test be made to ensure that the company is authorized to receive the requested data. For transaction level security, a mapping must be made to the specific user within a company and may be implemented either when the message arrives or before the response is returned by the Gateway.

- **Non-repudiation and intrusion alert** logging must be provided regardless of the point at which access control is exercised. It is recommended that the logging be done in a consistent fashion at both the Gateway and the data source.

- **Integrity** applies to guaranteeing that what arrives is identical to that which was sent and that only the intended recipients can access the contents. Encryption and access control combined with reliable transmission facilities will ensure that this goal is met.

6.1.2

In order to track information exchanges between CLECs and ILECs, audit trails of all transactions through the Gateway must be established.

Audit Trails are necessary to ensure the integrity of the information exchanged between the originating and responding parties. The audit trail must provide multiple functionality to support other functions related to OSS Access such as security, backup and recovery, Customer Interface Agreement compliance, and nondiscriminatory access proof.

It is recommended that an automated Audit Trail be established within the Gateway for all OSS access information exchanged between the CLEC and ILEC to provide proof that all Customer Interface Agreements have been met. The Audit Trail should provide the following functions:

- Transaction accounting at the Gateway - In order to track which CLEC sent a transaction across the Gateway, what was the transaction, who in the CLEC made the transactions, when it was made and how far the transaction went into the ILEC OSS, all transactions must be logged.
- The audit trail of transactions will be made available for viewing by each CLEC for its transactions and only its transactions.
- Changes to administrative data - If changes occur to a field on a customer record or if permission to change that field occurs, the audit trail must identify who made the change and when it was made.
- Detection of unscrupulous business practices and misuse - A scheme should be developed to identify if a CLEC or an ILEC attempts to block out other parties by overloading the Gateway with in-bound or out-bound traffic.
- Intrusion detection and attempts - If a CLEC or ILEC attempts to view or change a customer record without permission, the attempt must be logged in the audit trail.
- Proof that access is nondiscriminatory - The audit trail should be available to authorized parties in order to prove that traffic data are nondiscriminatory.
- Insurance of Customer Interface Agreements - The audit trail should be designed to provide proof that Customer Interface Agreements reached under Section 6.1.5 are met.

6.1.3.1

In order to comply with the FCC Order to provide nondiscriminatory access to OSS functionality, the CLECs and ILECs must reach a common understanding of specifically what functions are performed by the OSS and how they relate to their business processes.

The five major business areas defined in the FCC Order, (Pre-ordering, Ordering, Provisioning, Maintenance & Repair and Billing) will most likely not be performed in exactly the same manner or contain exactly the same data between any of the CLECs or ILECs. Therefore, it is imperative that a common understanding be reached of what business processes are being performed by the ILECs OSS and what data will be returned before a CLEC accesses the ILEC's OSS.

It is recommended that whenever possible a previously agreed upon and published definition for a business area function be used to describe that function.

6.1.3.2

The five major business areas defined in the FCC Order, (Pre-ordering, Ordering, Provisioning, Maintenance & Repair and Billing) will most likely contain similar terms in discussing data, but it is unlikely that these terms will mean exactly the same thing to every CLEC or ILEC. Therefore, before a CLEC accesses an ILEC's OSS functionality, the CLEC must understand the data terms (types, definitions, and attributes) of what they are requesting and what they will receive from the ILEC.

- Wherever possible, established standards from other references, such as American National Standards Institute (ANSI), OBF, Electronic Communications Implementation Committee (ECIC), T1M1, should be used to define these terms.
- If there is not an established standard definition for a particular data term, it should be developed by ATIS.
- A working agreement should be developed to pursue these definitions in an ongoing environment.

It is recommended that whenever possible a previously agreed upon and published definition for a business area data type be used to describe that data type.

6.1.3.3
The following is a list of American National Standards developed by Committee T1 that could be used in developing a common understanding of the Gateway:

- ANSI T1.214-1990 Generic Network Model for Interfaces between Operation Systems and Network Elements
    -
- ANSI T1.224-1992 Protocols for Interfaces between Operation Systems in Different Jurisdictions

- ANSI T1.246-1995 Information Model for Services for Interfaces Between Operations Systems Across Jurisdictional Boundaries to Support Configuration Management - Customer Account Record Exchange

- ANSI T1.228-1995 Services to Interface Between Operations Systems Across Jurisdictional Boundaries to Support Network Management (Trouble Administration)

- ANSI T1.227-1995 Extensions to Generic Model for Interfaces Between Operation Systems Across Jurisdictional Boundaries to Support Fault Management and for Standardized Protocol Interface (Called the “Q3” Interface in the TMN)

- ANSI T1.201-1993 Lower Layer Protocols for TMN Interfaces Between Operation Systems and Network Elements

- ANSI T1.208-1993 Upper Layer Protocol for TMN Interfaces

6.1.4
Because the performance of the Gateway system as a whole depends upon the aggregate performance of the subcomponents used to build the architecture; overall performance of Gateway systems must center upon providing comparable throughput and response time across each access method. These comparisons should be made between ILEC and CLEC for

transactions which are representative of the five core business functions between like modalities of architecture. A small CLEC choosing to implement network subcomponent access to the Gateway using a 9.6 modem dial-up should not expect the same performance of a CLEC who chooses to implement a DS-3 private line connection to the Gateway. Comparisons should be made to like modalities of access, security, and transaction architecture.

- A set of standard performance criteria should be developed by T1A1 that will initially seek to offer performance specifications for subcomponents of the Gateway and will guarantee minimum performance levels for each transaction type using specific subcomponents. These criteria should be established by testing and benchmarking.
- Unique performance requirements may be negotiated between CLECs and ILECs and documented in the bilateral agreements.
- A set of performance telemetry data for subcomponent types will be mutually agreed to and made known to all interested parties at a mutually agreed to frequency and granularity.

6.2.1
New service providers should participate in NIIF and Network Testing Committee (NTC)/IITP or equivalent Interoperability activities and when applicable perform the associated network level interoperability testing defined within the test plan.

To avoid potential problems related to synchronization and timing, new carriers follow the recommendations stated in section 5.1.2.5, section 5.2.2.5 and section 5.4.2.5 of the NRC II report "Network Reliability: The Path Forward," April 1996.

It is recommended that ATIS/NIIF or equivalent consensus based forum manage a database of relevant industry information that would assist new entrants in becoming aware of the availability of such information and how to obtain this information. The database could contain abstracts and pointers to information such as the NIIF interconnection template contained in the NIIF Network Operations Document (NOD) (formerly NOF Reference Document) and the new SS7 Cause Code Reference Manual contained in the NIIF NOD. (See Section 5.3.1.)

6.2.2
It is recommended that the NIIF should continue to place a high degree of focus on SS7 inter-network interconnection and interoperability by assuring adherence to, and providing clarification of, applicable standards. Industry participants should provide early detection and reporting of signaling network operational issues and performance information to the applicable NIIF group to help contribute to timely resolution and corrective action, thus improving network reliability.

It is also recommended that the planning process, as illustrated within the Planning Section of this document, be followed to ensure reliable signaling network interconnection and interoperability. (See Section 4.)

6.2.2.2
It is recommended that the Network Testing Committee (NTC) of the NIIF should initiate liaison with all identified parties (both public and private) chartered to develop LNP testing processes and procedures. These parties should be encouraged to participate in NTC activities to ensure synergies to enhance the identification and correction of signaling and other SS7 problems such as security and integrity of network management messages before they are introduced into the network. The NTC should encourage reports, white papers and/or common meetings so that individual test configurations, processes, procedures, and results could be shared.

6.2.3
New carriers, sponsoring new signaling network capability initiatives, should utilize the Service Planning Process, as defined within the Planning Section of this document, well in advance of deployment target dates so that the appropriate development process can be achieved. (See Section 4.)

The FCC may need to initiate timetables for compliance to provide features for new national or mandated services when it becomes clear that sufficient progress is not being achieved to reach the goals set by Section 256 of the Telecommunications Act of 1996.

6.2.4
It is recommended that signaling network test plans defined by the NTC be enhanced to include interconnectivity testing to verify minimum performance levels of signaling services provided by associated network elements including SSPs, STPs, and SCPs.

It is also recommended that standards bodies and service providers evaluate signaling network element (SSP, STP, and SCP) functionality in terms of transaction and link capacity and performance, operations, administration, maintenance, provisioning, database consistency and inter-network coordination, to determine the most efficient means of distributing or combining this functionality in network elements where appropriate per application. Signaling network architectural alternatives or enhancements to existing functional capabilities may be considered to relieve performance issues through more efficient utilization of network resources.

It is also recommended that T1A1 evaluate current performance measurements and make recommendations for additional measurements appropriate for the new multicarrier environment.

It is recommended that equipment providers be alert to the needs of the network and, in coordination with service providers, plan for network upgrade in a timely manner. Significant improvements in technology and the application of technology through the utilization of the proposed planning process should help alleviate this problem as the network evolves.

6.2.4.2
It is recommended that the appropriate standards bodies review the existing standards and request contributions to help define specifications for interconnectivity testing and tools where existing procedures are insufficient.

It is also recommended that the FCC review the progress of this activity and set timetables, if appropriate, for implementation of a set of internetwork fault diagnostic procedures.

6.2.5
It is recommended that the NIIF expand the Bilateral Interconnection Template (NIIF Issue 0014) to reflect the Security applicable best practices, standards (Committee T1), base guidelines (e.g., NIIF Network Operations Document Section 9) and Data Connection Trust Agreements.

It is also recommended that the appropriate standards groups, service providers and equipment suppliers be strongly encouraged to apply the recommendations from NRC II as they relate to security issues with particular emphasis on firewalls.

6.2.5.2
It is recommended that T1S1 and/or T1M1 be requested to investigate this issue and provide additional Gateway firewall specifications and recommendations that would detect and report the existence of potential unauthorized signaling activity.

6.2.6.1
It is recommended that T1S1 should be solicited for contributions to the NIIF for formulation of Data Connection Trust Agreements (as shown in Section 6.7) and other solutions to this problem.

It is recommended that standard bodies should be requested to solicit recommendations to outline areas of improvement and provide recommendations (issue standards as required) to improve network interconnect robustness.

6.2.6.2
It is recommended that T1S1 solicit contributions that fully define the looping message issue and that address a comprehensive set of functions that ensure against this reliability risk.

6.2.6.3
It is recommended that a carrier’s interconnection template should ensure that signaling link diversity is established and maintained, preferably by an automated process.

It is also recommended that NIIF investigate signaling link diversity issues and provide recommendations for an automated process to ensure long-term integrity of signaling link diversity.

6.2.6.4
It is recommended that interconnected service providers establish and maintain coordination administrators who ensure, by implementing defined notification rules, maintenance activities by both parties do not jeopardize signaling network reliability.

It is also recommended that the administration of maintenance activities that affect two or more service providers should follow rules negotiated before service initiation and incorporated within bilateral service agreements.

6.2.6.5
It is recommended that NANC continue to address issues related to local number portability databases, ensuring timely number distribution and ensuring data consistency across all associated LNP databases.

It is recommended that T1S1 address signaling network architectural issues related to the query of the LNP databases to reduce the instance of looping messages due to inconsistent data in multiple databases and to minimize or eliminate any adverse signaling network traffic that would cause reliability risks.

6.3.1
The broad spectrum of services should be categorized by T1A1 into subsets for which interoperability performance measures can be specified that are reasonable and recognizable to the participants.

- From the FCC perspective, the categorizations should be such that… major outages of service and deterioration in the overall service levels of the industry [can be identified].

- From the Service Provider perspective, such categorizations for use in negotiating their interoperability arrangements will naturally evolve as part of the standards process.

- From the Service Consumer perspective, such categorizations present a new level of challenge. The categorizations and measures, to be most effective, require the service providers' commitment to the monitoring and reporting of performance. Such commitments may evolve through consumer advocacy groups.

The first set of services that should be considered are those that impact the greatest number of customers…. The service subset should now be expanded to include facilities such as signaling interconnection Gateways and backbone facilities for all providers, including those facilities that support the cable TV industry and wireless service providers. Both frequency of failure and length of failure indices should be established. Reporting of these indices should be supported by performance monitoring data supplied by the appropriate communications components.

It is recommended that standard bodies such as T1A1 should establish the services to be measured and determine how they should be measured. Industry participation by all service providers and equipment vendors should be encouraged by the FCC.

6.3.2
Specific agreements between service providers will determine the continuance of a trusted relationship between industry partners. A checklist of items to ensure service levels are maintained that can be included in the agreements between industry partners is available in the

interoperability templates developed for NRC II and updated for NRIC. Performance monitoring parameters should be identified for critical items that impact the ability of interconnecting parties to complete their normal business activity.

Performance measures for operational access should include measurements designed to monitor occurrences of system access congestion including root cause analysis.

6.3.3

All interconnecting parties (established and new) should specify in their interconnection agreements the parameters to be monitored to maintain normal business activity and pre-agree to the triggers and actions to be taken if those parameters go out of bounds.

Work in existing standards bodies and industry forums on network reliability performance measures should be extended to facilitate its application in new segments of the voiceband services telecommunications industry (cellular, satellite, cable TV, CLECs and ILECs). This work will adapt measures such as the outage index of existing measures to clarify their application to these other segments and also to suggest ways in which selective exchange of these measures can better assess the impact of outages within one segment on the other segments it is connected to.

The existing templates for reliability and interconnection criteria [NRC II template] and interconnection templates [Network Operations Forum (NOF) draft handbook for interconnection between LECS] should continue to be refined and updated to reflect the rapidly evolving telecommunications environment. These changes will facilitate highly reliable customer services in future, more fully interconnected networks.

Based on the recommendations made earlier in this section, it is expected that T1A1.2 and NIIF would define specific service subsets and thresholds for use in performance monitoring. These performance monitoring items would apply across the industry. Once these service subsets and thresholds are identified, ATIS NRSC should then recommend specific performance monitoring items that could be reported by the industry and formally tracked by the FCC and other regulatory agencies.

6.4.4

It is recommended that the NIIF expand the Bilateral Interconnection Template (NIIF Issue 0014) to reflect the Security applicable best practices, standards (Committee T1), base guidelines (e.g., NIIF Network Operations Document Section 9) and Data Connection Trust Agreements (See Operations Section 6.7.4 Sample Data Connection Agreements, page 65). It is further recommended that the ATIS Network Reliability Steering Committee expand the Outage Reporting Cause Code fields better capture security related agents and problems.

It is recommended that the NIIF expand its reliability efforts to address gateway security screening against harmful messages and spoofing (deliberate insertion of false or misleading messages or message content). It is also recommended that the appropriate standards groups, service providers and equipment suppliers be strongly encouraged to apply the recommendations

from NRC II as they relate to security issues with particular emphasis on firewalls, harmful code detection and mediated access.

It is recommended that affected carriers and vendors reinforce their defensive, detective and reactive fraud detection and network security capabilities and resources to deal with the increased risk and provide additional training, tools and participation in at least two industry fora such as the ATIS Toll Fraud Prevention Committee, the NSTAC Network Security Information Exchange and the Forum for Incident Response and Security Teams (FIRST).

It is recommended that Service Providers and equipment suppliers test for security conformance. Every effort should be made to see if security can be included in the interoperability and stress testing done by the NTC/IITC.

It is recommended that ATIS expand the charter of the Toll Fraud Prevention Committee TFPC to address network security. It is also recommended that the industry support ATIS and actively participate in the expansion of the TFPC.

6.4.5

The industry and the Commission will need to pay continuing attention to security risks as they continue to develop in the new environment. Special attention should be paid to the following areas:

- **Standards** e.g., ATIS NIIF (NOF) Reference Document Section III, Subsection 9, Network Security Base Guideline, and ANSI T1 233-1993, ANSI T1.243-1995 and ANSI T1.252-1996 Telecommunications OAM&P Security Framework, Baseline Security Requirements for Telecommunications Management Networks (TMN) and TMN Directory, and additional T1 standards for partitioned access control and firewall within a TMN Gateway environment

- **Access Control, and Audits:** e.g., Access Control Lists and Data Connection Agreements to facilitate secure open market electronic commerce

- **Firewalls** e.g., STP Gateway Screening, Near Network Element Concept, Closed-User Groups, Proxy Servers, Internet Firewalls, FrameRelay Firewalls and Encryption, Connectionless Security Features of SMDS, *etc.*

- **Authentication** e.g., Strong, Robust,, User Friendly, Open Standards Based and Manageable like RADIUS

- **Reporting** of security related reliability impacting incidents and outages.

- **Intrusion Detection** and containment through cooperating security points of contact referral and enforcement of the Data Connection Agreement(s)

6.5.1
The NRIC continues to endorse the value of industry-wide interoperability testing and funding; and encourages ATIS to accelerate the implementation of the NCR II recommendations by 3Q97.

6.5.2
The NRIC recommends to ATIS that the first priority of the new NTC/IITC should be confirmation of the interoperability of LNP; making full utilization of all current field tests. In addition, NTC/IITC should investigate the interaction of the various databases that will be associated with LNP as well an assessment of the security of sensitive information and minimum performance levels.

6.5.3
The NIIF should be encouraged to identify the tests that need to be performed in the next 18 months as soon as possible. Special consideration should be given to interoperability tests of unbundled network elements, wireline/wireless integration, and location oriented local number portability.

6.5.4
The IITC Oversight Group… [should be asked to identify] the current activities of other industry associations relative to interoperability to maximize the efficiency of the interoperability testing effort.

6.5.5
The NIIF under ATIS should be asked to develop a minimum set of scripts for acceptance testing to assure that interconnected networks are working properly before they are activated for live traffic.

7.1.2.1
The industry should closely monitor the proliferation of industry associations and fora involved with access standards development to guard against the negative effects associated with the decentralization of standards development. It is important to acknowledge that these groups have had an extremely positive effect on standards development, to date. If the industry determines in the future that the quality or effectiveness of standards is being compromised, or the timeliness of the standards development process is being adversely affected, then the industry should consider forming a special end-user focused task group to address this matter.

….Industry fora that include users as integral members and contributors (such as ATM Forum, North American ISDN Users' Forum, and the Intelligent Network Forum) should be encouraged to allow users the opportunity to actively participate and influence standards development. The standards definition procedure should be made available to all stakeholders in the industry in order to hear all points of view. It is also important to recognize that industry fora can have a detrimental effect on the standards development process if stakeholders engage in "forum shopping" to participate in fora or establish new fora that support their needs. To date, the

benefits of these industry fora to users have outweighed the negative effects on the overall process.

….[C]ompetitive forces will drive Bellcore or other industry fora to develop generic requirements. It is critical that whatever group develops such requirements, the process be open and reasonably available for participation by all interested parties.

As suggested in the NRC II report, to expedite the standards development process, interactive electronic access methods should be employed and a schedule with milestones and deliverables employed…. [T]o improve compatibility, standards should have a sharp technical focus and standards bodies should strive to minimize the complexity and optionality of requirements. At the same time, standards should focus on achieving a basic level of interoperability, and should not be so specific as to stifle innovative approaches to a problem. The development of baseline standards will ensure that network elements can accomplish their basic function without impairing the network, and that user-to-user functionality will be achieved.

….It would also be beneficial to create a facility for various groups to test interoperability in a captive network, and in a low profile environment that allows engineers to communicate to resolve interoperability issues.

7.1.2.2
The Council recommends that the FCC develop a short list of nationally accepted services and require that no telecommunications service provider make any system-wide changes in or extensions to such services that would cause a subscriber to lose such services unless those changes or extensions (1) are the product of the National Planning Process discussed in Section 4 above and (2) provide an opportunity to the customer to maintain uninterrupted service.

7.1.2.3
Performance monitoring and testing efforts within the industry, already acknowledged and accepted by the FCC, should continue under ATIS and are discussed further in Section 7.3 of this report. No additional oversight is required.

7.1.2.4
No additional action is required to address increased response time and call suspension issues associated with increased interconnections. NRC II recommendations are adequate.

7.1.2.5
Billing issues are being addressed under ATIS. No further action is required.

7.1.2.6
If third party access to Intelligent Network components is extended to include the user community, the industry should develop a template (see Section 7.5) to allow for the successful passing of call handling data.

7.2.3.1

The existing market interactions and standards process should proceed until… [technologies offered to users by carriers that offer transmission rates of higher than T1 (1.544 Mbit/s)] are widely enough deployed to make it possible to determine what issues become important. If these are not already under study in the various standards and industry bodies when that occurs, they should be referred at that time by industry contribution. The government should legislate a solution only where it appears voluntary action is not meeting a compelling national need for interoperability.

7.2.3.2
To guard against undesired interference, the FCC should continue oversight under Part 68 of new technologies applied to unbundled loops.

7.3.3.1
The telecommunications industry should maintain the voluntary standards process.
The private sector has created an extensive framework of standards-setting activity based on voluntary collaboration. The FCC need not assert its regulatory influence in this process other than to assure that standards continue to be set quickly and be created in a way that helps stimulate competition and innovation.

7.3.3.2
The telecommunications industry must take action to ensure CPE interoperability.
As no standards body enforces its standards, other means of assuring compliance is required. The dictates of the dominant local exchange carrier had been the primary mechanism through which this goal was achieved in the past but cannot be relied on to play this role in a competitive environment. In the network of networks a new mechanism must be found. The free market is a potential, but inefficient ad hoc processes could jeopardize public safety if used as the sole mechanism for assuring CPE interoperability. To that end the NRIC encourages the industry to create a CPE interoperability program for the FCC's list of national services as outlined in other sections of this report. One way to do this would be to request that ATIS extend the charter of the IITC beyond network to network interoperability testing, and include network to CPE interoperability testing for the list of essential FCC services. ATIS could possibly model a public network certification program after that being used in the cellular sector or the computer networking industry. The industry could ask ATIS to establish a certification seal for the essential services required for public safety along with the interoperability criteria. Private sector test laboratories could then conduct certification tests as a necessary criterion for FCC Part 68 registration. In addition, there should be a program of manufacturer self-declaration to the interoperability criteria.

7.3.3.3
Standards extensions must be tolerated to stimulate innovation. In prescribing a means of ensuring CPE interoperability for public safety in the network of networks, it is equally important to protect the source of innovation represented by CPE and its interaction with the network. To that end the FCC should explicitly express its position regarding extensions to the standards for CPE interconnection to the network. Criteria for such tolerance should include preservation of

basic interoperability for public safety, competitive fairness, and any other matters of public interest.

7.4.2
A crucial step in eliminating barriers to interoperability is to establish a document expanding on current Network Disclosure statements that clearly and precisely define the technical criteria and standards to be met by CPE and network equipment manufacturers when building a device for a particular type of Network-to-CPE interconnection. A document in the form of a specifications template has been developed that serves as a guideline for Network-to-CPE interconnection. This template, located at the end of Section 7.4, categorizes and briefly describes technical specifications that may be useful in building a Network-to-CPE interconnection.

7.5.2.1
The NRIC recommends to vendors that, for each interface their product lines support and at which interoperability is required, the interface specifications should be made publicly available, although such interfaces need not necessarily be standardized. However, where strict interoperability is essential, vendors should work together with TIA engineering committees and Committee T1 in order to choose from the existing standards or develop new standards to specify such interfaces. Once defined, such standards and the corresponding interfaces should be made publicly available. All relevant standards should be made easier to obtain and use.

7.5.2.2
For national services, a basic level of connectivity must be ensured for each CPE. For more local services, competitive features, additional to the basic level of connectivity may be allowed…. At… [the basic] level, the associated standard should be as simple as possible, allow no options and be based on the best available technical solution…. If vendors are to provide interoperability at… [a] higher level, they would need to agree among themselves on a common set of features and tests, and specify the additional conditions for interoperability.

7.6.2
The recommendations of … [the NRC II Advanced Intelligent Network Subteam] should be followed…. The specific recommendations can be found in the February 22, 1996 "Network Reliability Council (NRC), Reliability Issues - Changing Technologies Focus Group, Advanced Intelligent Network Subteam Final Report." The following are the specific references to the recommendations…:

- Service Creation/Provisioning Process, Section 5.4 < Recommendation 18 >
- Interoperability, Section 5.5 < Recommendations 19, 20 >
- AIN Network Overload Controls and SCP Capacity and Overload, Section 5.6
- < Recommendations 21,22, 23, 24 >
- SSP/SCP Testing, Section 5.8 < Recommendations 26, 27 >
- Mediation & Third Party Service Provider Access, Section 5.9 < Recommendations 28, 29 >

8.3.1

ISPs and telecommunications carriers should establish a performance measurement program to assess and monitor the interconnections between the PSTN and ISPs…. This could include measures such as calls blocked at the terminating switch, calls blocked at the inter-office trunk level, and dial tone delay. A template is described in section 8.4 which could serve as the basis for establishing such measures.

….If it is determined ISPs and telecommunications carriers are not able to work together to establish standard measurements and carry out joint planning, the FCC may consider whether ISPs constitute a special class of end user which should receive treatment or services not available to non-ISP end users. The FCC would need to define precisely the characteristics that define an ISP and possibly create some kind of registration process for ISPs which meet the Commission's criteria.

8.3.2
ISPs and telecommunications carriers should develop protocol standards for the exchange of control and accounting information in a standardized and reliable way.

8.3.3
ISPs and telecommunications carriers should develop mutually beneficial network management interface standards such that both PSTN and ISP network operators can monitor the performance of appropriate elements of each other's networks.

8.4
A requirements template has been developed that serves as a guideline for Internet interconnection. This template categorizes and briefly describes the technical specifications necessary to connect networks to ISPs.

9.1.2.1[1]
Use of a Network Interface Specification template is advised when a new network interface is identified for standardization. Standards bodies should use this type of template in developing the initial Standards Project Plan(s) for new interfaces to address the relevant important areas for interconnection reliability. An example template for standards development planning is contained in Section 9.2.

9.1.2.1[2]
Industry associations, such as ATIS and TIA, should consider the value of incorporating performance requirements for complex network elements with the interface standards requirements. Also, the associations should consider how such requirements should be developed and funded.

9.1.2.1[3]
Wherever appropriate, standards bodies should work with other industry groups that use standards, such as the ATM Forum, to more precisely define standards requirements and minimize complexity and optionality. Excessive optionality can be dealt with through an appropriate contribution to the affected standards committee or forum. A Network Interface

Specification, such as the example contained in Section 9.2 of this report, should also be used by industry forums to further define, detail and approve implementation for the industry.

9.1.2.3[4]
New network providers are encouraged to participate in existing telecommunications industry standards processes, either directly or through associations, via membership or contributions to Committee T1 or TIA.

9.1.2.3[5]
Where adequate network interface standards exist, suppliers should develop and evolve their products to meet those standards. If interface standards are not yet established, network service providers and network equipment suppliers should be encouraged by the FCC to actively participate in the development of robust network interface standards to accelerate their availability.

9.1.2.3[6]
Interconnecting network providers should utilize industry-proven interconnection standards.

9.1.2.3[7]
While standards are generally voluntary, increased emphasis should be placed on the value of compliance in ensuring network interoperability and reliability. However, in the case of public safety concerns, standards are identified with a "mandatory" emphasis.

9.1.2.4[8] The most effective means to accelerate the standards development process is to ensure new standards work has sharp technical focus and clear standards deliverables, plus final and interim milestones for those deliverables. Exhibits 6 and 7 from NRC II contain information on standards project proposals and project tracking based on this recommendation.

9.1.2.4[9]
All telecommunications standards bodies, accredited and non-accredited SDs, should implement by year end 1997 interactive electronic access methods to expedite the submission, creation, acceptance, review and finalization of technical standards. This is already underway, but a completion date for all organizations has not been specified.

9.1.2.4[10] The Forum Process should be employed by the industry and companies/agencies to foster innovation and to produce contributions to the development of standards, not in lieu of standards. Industry forums have been instrumental in specifying implementation agreements.

9.2.2

The NRIC-3 Focus Group 2 on Standards-Setting, which is focused primarily on the process and roles of standards development organizations, recommends several modifications to the template [originally developed by the NRC-2 Network Interconnection Focus Group 2]. These modifications reflect the view that while all items listed in this template should be considered by affected service providers to establish and maintain interconnection, some items may not typically fall under the purview of standards-setting organizations. It should also be

noted that other organizations may find the processes that evolve from this template useful and are encouraged to make use of and enhance it.

9.3.2 It is recommended that the NRC II document Section 12, Exhibit 2, be re-titled "Key Telecommunications Standards Related Groups", and be modified as… [shown in Section 9.3.2].

9.4.2.1
When it is determined that a formal technical specification is needed to establish a telecommunications interconnection arrangement the following steps should be taken:

- Conduct a search to determine if an existing standard will satisfy the technical need and apply it.

- If the technical need can not be met by an existing standard, develop a high-level description and submit it to the (open and public) standards developer charged to develop the type of interconnect standard needed.

- If either of the above two steps can not be performed due to a lack of knowledge about standards or the standards process, contact the American National Standard Institute (ANSI) Information Infrastructure Standards Panel (IISP) for advice.

CONTACT: Peter Lefkin Phone 212 642 4979
Internet: PLEFKIN@ansi.org

9.4.2.2 Standards developers should take steps to assure continuous improvement in their development and delivery processes. This should include the continued improvement and utilization of the Internet and the Web to advertise work programs, progress, and accomplishments.

Specific to the needs of Section 256, it is recommended that each standards developer establish a mechanism to support informal communications with the FCC to:

- provide key tracking information on standardization activity related to the interconnection requirements of Section 256. The set of tracking information should include existing standards, standards under development and proposed work on new standards that may be related to the FCC's *First Report and Order In the Matter of Implementation of the Local Competition Provisions in the Telecommunications Act of 1996 and Interconnection between Local Exchange Carriers and Commercial Mobile Radio Service Providers,* CC Docket Nos. 95-185 and 96-98 (August 8, 1996), Sections 212 and 366:

    - Six technically feasible interconnection points:
        - the line-side of a local switch;
        - the trunk-side of a local switch;

- the trunk interconnection points for a tandem switch;
- central office cross-connect points;
- out-of-band signaling transfer points; and
- the points of access to unbundled elements.

- Seven unbundled network elements:
  - access to local loops;
  - network interface devices;
  - local and tandem switching capability;
  - interoffice transmission facilities;
  - signaling and call-related databases;
  - operations support systems functions; and
  - operator services and directory assistance facilities.

- provide a documented process internal to the SD for review of concerns raised about standardization activities expressed by materially affected parties to be related to the goals of Section 256;

- provide a duly appointed or elected FCC liaison officer to oversee related standards development activities related to Section 256 and other laws, and to provide a single point-of-contact on all related standardization issues.

9.4.3[3] It is recommended that the FCC commit sufficient resources to provide:

- a single point-of-contact for the informal exchange of information between the FCC and standards developers on activities related to the interconnection requirements of Section 256;

- ongoing monitoring of standardization activities via the Internet and Web and, as required, through direct monitoring of key interconnection standardization activities at meetings.

9.4.3[4] The FCC may wish to continue an oversight role to address any issues that come before it on a complaint basis if some party believes that the standards process is not adequate to address their needs. In the first instance, the FCC should seek to have disputes resolved by manufacturers, service providers and/or end users; if they cannot resolve the issue, the FCC may need to get involved in the dispute.

10.1.2 [1] …. [T]he current procedures in place at ANSI, IISP, TIA, EIA, Committee T1, and other SDs, both domestically and internationally, are adequate to capture standards needs and provide input to the standards process when these procedures are utilized by groups representing persons with disabilities. More active participation by groups representing persons with disabilities in the standards process is encouraged including submission of contributions and comments on the draft standards when they go through the public review period. Such groups should also become active in the ANSI Consumer Interest Council.

10.1.2[2] SDs should include a step in the establishment of new work that draws attention to the needs of individuals with disabilities.

10.1.2[3] SDs should notify the FCC of any new standardization work that may impact individuals with disabilities.

10.1.2[4] The FCC should encourage the existing outreach programs to continue and join with industry in sponsoring human resource training programs that provide guidance to equipment designers about the wide range of accessibility needs of persons with disabilities. As new technologies become available to facilitate accessibility the FCC should monitor such developments and provide public notice of such innovations.

10.1.2[5]
On the regulatory side, the FCC will need to conclude its Inquiry under Section 255 and take whatever actions it deems appropriate under Section 256. The cooperative activities of the Telecommunications Access Advisory Committee ("TAAC") have demonstrated how industry and consumer groups can work together to solve accessibility problems and achieve a high degree of consensus. The Commission should work closely with the Access Board as it develops its Guidelines and provide the FCC's guidance and recommendations from the record created in response to the FCC's Inquiry in WT Docket No. 96-198.

10.1.2[6]
On the voluntary standards side, Focus Group 2 recommends that the FCC follow the recent guidance given by Congress to all federal agencies in the National Technology Transfer and Advancement Act of 1996 ("NTTAA"). In addition it recommends that the FCC utilize voluntary standards for regulatory purposes and participate directly in the standards creating process.

10.1.2[7]
By direct participation in the standards process, where appropriate, the FCC can bring its wisdom and insights directly to the SDs. At a minimum, the FCC may wish to reserve an oversight role to address any issues that come before it on a complaint basis if some party believes that standards being generated are not adequate to address its needs. In the first instance, the FCC should seek to have disputes resolved by manufacturers and service providers and only involve the FCC in the event the matter can not be resolved. This approach would also be in keeping with other Congressional guidance in another area, where in the Communications Assistance for Law Enforcement Act of 1994, Congress again deferred to the voluntary, consensus standards process, and limited the FCC's role to one of oversight if some party believed the resultant industry standard was in some manner deficient.

11.1.2[1]
The FCC and the rural telephone industry should work together to educate all telecommunications providers about where and how different types of standards are developed.

The FCC and the industry should jointly sponsor a seminar(s) explaining how rural carriers can participate in standards development.

11.1.2[2]
The FCC is encouraged to monitor the standards process so they remain informed about the activities taking place in the standards forums.

11.1.2[3]
The FCC should encourage all standards bodies to allow telecommunications providers to access information regarding developing standards and provide input to standards via telecommunications.

11.1.2[4]
The FCC may wish to continue an oversight role to address any issues that come before it on a complaint basis if some party believes that the standards process is not adequate to address their needs. In the first instance, the FCC should seek to have disputes resolved by manufacturers, service providers and/or end users; if they cannot resolve the issue, the FCC may need to get involved in the dispute.

13. GLOSSARY OF ACRONYMS

ADA	Americans with Disabilities Act
ADSL	Asymmetrical Digital Subscriber Line
AIN	Advanced Intelligent Network
ALTS	Association for Local Telecommunications Services
ANSI	American National Standards Institute
APA	Administrative Procedures Act
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
ATM OAM	Asynchronous Transfer Mode Operations Administration and Maintenance
ATSC	Australian Telecommunications Standardization Committee
ATU-R	Asymmetrical Termination Unit-Remote
BGP	Border Gateway Protocol
BOC	Bell Operating Company
BRI	Basic Rate Interface
CABS	Carrier Access Billing System
CALEA	Communications Assistance for Law Enforcement Act
CAP	Carrierless AM/PM
CAP	Competitive Access Provider
CCS	Common Channel Signaling
CCT	Consultative Committee Telecommunications
CDMA	Code Division Multiple Access
CEMA	Consumer Electronics Manufacturers Association
CIC	Consumer Interest Council
CITEL	InterAmerican Telecommunications Commission
CLC	Carrier Liaison Committee
CLEC	Competitive Local Exchange Carrier
CMIP	Common Management Information Protocol
CMISE	Common Management Information Services Element
CNRI	Center for National Research Initiatives
COMPTEL	Competitive Telecommunications Association
COPOLCO	Consumer Policy Committee
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CSA	Canadian Standards Association
CTIA	Cellular Telecommunications Industry Association
DCC	Data Communications Channel
DID	Direct Inward Dialing
DMT	Discrete Multitone

DOD	Department of Defense
DOJ	Department of Justice
DOT	Department of Transportation
ECIC	Electronic Communications Implementation Committee
EDH	Electronic Document Handling
EDI	Electronic Data Interchange
EEOC	Equal Employment Opportunity Commission
EIA	Electronic Industries Association
EIA CEMA	EIA Consumer Electronics Manufacturers Association
EIF	Electronic Industries Foundation
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Enhanced Services Provider
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FDDI	Fiber Distributed Data Interface
FR	Frame Relay
GII	Global Information Infrastructure
GSA	General Services Administration
GSC	Global Standardization Collaboration
GSM	Global System for Mobile Communications
GTT	Global Title Translation
HAC	Hearing Aid Compatible
HACNRC	Negotiated Rulemaking Committee addressing Hearing Aid Compatibility
HHS	Health and Human Services
HPC	High Probability of Completion
I/O	Input/Output
IAB	Internet Architecture Board
IC	Interexchange Carrier
ICCF	Industry Carriers Compatibility Forum
IEC	Interexchange Carrier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IILC	Information Industry Liaison Committee
IISP	Information Infrastructure Standards Panel
IITC	Internetwork Interoperability Testing Committee
IITP	Internetwork Interoperability Test Plan
ILEC	Incumbent Local Exchange Carrier
IN	Intelligent Network
INC	Industry Numbering Committee

IP	Internet Protocol
IPR	Intellectual Property Rights
ISDN	Integrated Services Digital Network
ISO	International Standardization Organization
ISOC	Internet Society
ISP	Internet Service Provider
ISUP	Integrated Services Digital Network User Part
ITI	Information Technology Industry Council
ITU	International Telecommunication Union
IXC	Interexchange Carrier
JTC	Joint Technical Committee
KDC	Key Distribution Center
LAN	Local Area Network
LEC	Local Exchange Carrier
LERG	Local Exchange Routing Guide
LIDB	Line Information Data Base
LNP	Local Number Portability
LRN	Local Routing Number
LSR	Local Service Request
LSSGR	LATA Switching System Generic Requirements
MDF	Main Distribution Frame
MRVT	MTP Route Verification Test
MTTR	Mean Time to Repair
NAFTA	North American Free Trade Agreement
NANC	North American Numbering Council
NANP	North American Numbering Plan
NANPA	North American Numbering Plan Administrator
NCITS	National Committee for Information Technology Standards
NCLD	National Center for the Law and Deaf
NCS	National Communications System
NCTA	National Cable Television Association
NE	Network Element
NEPA	National Environmental Policy Act
NI OMAP	Network Interconnect Operations, Maintenance, Administration Part
NIA	Network Interconnection/Architecture Committee
NIC	National ISDN Council
NID	Network Interface Device
NII	National Information Infrastructure
NIIF	Network Interconnection and Interoperability Forum
NIMC	Network Installation and Maintenance Committee
NIST	National Institute of Standards and Technology
NMC	Network Management Committee

NMF	Network Management Forum
NOD	National Office on Disabilities
NOD	Network Operations Document
NOF	Network Operations Forum
NRC	Network Reliability Council
NRIC	Network Reliability and Interoperability Council
NRRIC	Network Rating and Routing Information Committee
NRSC	Network Reliability Steering Committee
NS/EP	National Security and Emergency Preparedness
NSIE	Network Security Information Exchange
NSSN	National Standards System Network
NSTAC	National Security Telecommunications Advisory Council
NTA	National Telecommunications Alliance
NTC	Network Testing Committee
NTCA	National Telephone Cooperative Association
NTIA	National Telecommunications and Information Administration
NTTAA	National Technology Transfer and Advancement Act
OAM&P	Operations, Administration, Maintenance, and Provisioning
OBF	Ordering and Billing Forum
OC	Optical Carrier
OMAP	Operations, Maintenance, Administration Part
OMB	Office of Management and Budget
ONA	Open Network Architecture
OPASTCO	Organization for the Promotion and Advancement of Small Telecommunications Companies
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OSS	Operations Support Systems
OTG	Operations Task Group
OTGR	Operations Technology Generic Requirements
PAS	Publicly Available Specifications
PCIA	Personal Communications Industry Association
PCS	Personal Communications Services
PDH	Plesiochronous Digital Hierarchy
PN	Project Number
PPP	Point to Point Protocol
PRI	Primary Rate Interface
PSN	Public Switched Network
PSO	Participating Standards Organization
PSTN	Public Switched Telephone Network
PTG	Planning Task Group
PTN	Public Telephone Network
PVA	Paralyzed Veterans Association

QOS	Quality of Service
RAST	RAdio STandardization
RCF	Remote Call Forwarding
RLAN	Radio Local Area Network
S/MIME	Secure Multipurpose Internet Mail Extensions
SBCA	Satellite Broadcasting and Communications Association
SCCP	Signaling Connection Control Part
SCE	Service Creation Element
SCP	Service Control Point
SCTE	Society of Cable Telecommunications Engineers
SD	Standards Developer
SIA	Satellite Industry Association
SIF	SONET Interoperability Forum
SKAM	Skills, Knowledge, Access, and Motive
SNAC	Service Management 800 Number Administration Committee
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SP	Standard Proposal
SPPM	Services Planning Process Model
SRVT	SCCP Route Verification Test
SS7	Signaling System 7
SSL	Secure Socket Layer
SSP	Signaling Switch Point
STAR	Standards and Technology Annual Report
STP	Signaling Transfer Point
T1AG	T1 Advisory Group
TA96	Telecommunications Act of 1996
TAAC	Telecommunications Access Advisory Committee
TCIF	Telecommunications Industry Forum
TCP/IP	Transmission Control Protocol/Internet Protocol
TDD	Telecommunications Devices for the Deaf
TDM	Time Division Multiplexed
TDMA	Time Division Multiple Access
TFPC	Toll Fraud Prevention Committee
TIA	Telecommunications Industry Association
TMN	Telecommunications Management Network
TRA	Traffic Routing Administration
TSACC	Telecommunications Standards Advisory Council of Canada
TSB	Telecommunications Systems Bulletin
TTA	Telecommunications Technology Association of Korea
TTC	Telecommunication Technology Committee
USPS	U.S Postal Service
USTA	United States Telephone Association

VAN	Value Added Network
WDM	Wavelength Division Multiplexing

14. APPENDICES

APPENDIX A

47 U.S.C.A. s 256

UNITED STATES CODE ANNOTATED
TITLE 47. TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS
CHAPTER 5--WIRE OR RADIO COMMUNICATION
SUBCHAPTER II--COMMON CARRIERS
PART II--DEVELOPMENT OF COMPETITIVE MARKETS

s 256. Coordination for interconnectivity

(a) Purpose

It is the purpose of this section--

(1) to promote nondiscriminatory accessibility by the broadest number of users and vendors of communications products and services to public telecommunications networks used to provide telecommunications service through--

(A) coordinated public telecommunications network planning and design by telecommunications carriers and other providers of telecommunications service; and

(B) public telecommunications network interconnectivity, and interconnectivity of devices with such networks used to provide telecommunications service; and

(2) to ensure the ability of users and information providers to seamlessly and transparently transmit and receive information between and across telecommunications networks.

(b) Commission functions

In carrying out the purposes of this section, the Commission--

(1) shall establish procedures for Commission oversight of coordinated network planning by telecommunications carriers and other providers of telecommunications service for the effective and efficient interconnection of public telecommunications networks used to provide telecommunications service; and

(2) may participate, in a manner consistent with its authority and practice prior to February 8, 1996, in the development by appropriate industry standards-setting organizations of public telecommunications network interconnectivity standards that promote access to--

(A) public telecommunications networks used to provide telecommunications service;

(B) network capabilities and services by individuals with disabilities; and

(C) information services by subscribers of rural telephone companies.

(c) Commission's authority

Nothing in this section shall be construed as expanding or limiting any authority that the Commission may have under law in effect before February 8, 1996.

(d) Definition

As used in this section, the term "public telecommunications network interconnectivity" means the ability of two or more public telecommunications networks used to provide telecommunications service to communicate and exchange information without degeneration, and to interact in concert with one another.

APPENDIX B

7 U.S.C.A. s 251

UNITED STATES CODE ANNOTATED
TITLE 47. TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS
CHAPTER 5--WIRE OR RADIO COMMUNICATION
SUBCHAPTER II--COMMON CARRIERS
PART II--DEVELOPMENT OF COMPETITIVE MARKETS

Current through P.L. 105-4, approved 3-3-97

s 251. Interconnection

(a) General duty of telecommunications carriers

Each telecommunications carrier has the duty--

(1) to interconnect directly or indirectly with the facilities and equipment of other telecommunications carriers; and

(2) not to install network features, functions, or capabilities that do not comply with the guidelines and standards established pursuant to section 255 or 256 of this title.

(b) Obligations of all local exchange carriers

. . . .

APPENDIX C

47 U.S.C.A. s 255

UNITED STATES CODE ANNOTATED
TITLE 47. TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS
CHAPTER 5--WIRE OR RADIO COMMUNICATION
SUBCHAPTER II--COMMON CARRIERS
PART II--DEVELOPMENT OF COMPETITIVE MARKETS
Current through P.L. 105-4, approved 3-3-97

s 255. Access by persons with disabilities

(a) Definitions

As used in this section--

(1) Disability

The term "disability" has the meaning given to it by section 12102(2)(a) of Title 42.

(2) Readily achievable

The term "readily achievable" has the meaning given to it by section 12181(9) of Title 42.

(b) Manufacturing

A manufacturer of telecommunications equipment or customer premises equipment shall ensure that the equipment is designed, developed, and fabricated to be accessible to and usable by individuals with disabilities, if readily achievable.

(c) Telecommunications services

A provider of telecommunications service shall ensure that the service is accessible to and usable by individuals with disabilities, if readily achievable.

(d) Compatibility

Whenever the requirements of subsections (b) and (c) of this section are not readily achievable, such a manufacturer or provider shall ensure that the equipment or service is compatible with existing peripheral devices or specialized customer premises equipment commonly used by individuals with disabilities to achieve access, if readily achievable.

(e) Guidelines

Within 18 months after February 8, 1996, the Architectural and Transportation Barriers Compliance Board shall develop guidelines for accessibility of telecommunications equipment and customer premises equipment in conjunction with the Commission. The Board shall review and update the guidelines periodically.

(f) No additional private rights authorized

Nothing in this section shall be construed to authorize any private right of action to enforce any requirement of this section or any regulation thereunder. The Commission shall have exclusive jurisdiction with respect to any complaint under this section.

APPENDIX D

CHARTER FOR THE NETWORK RELIABILITY AND INTEROPERABILITY COUNCIL

A. The Committee's Official Designation

The official designation of the advisory committee will be the "Network Reliability and Interoperability Council."

B. The Committee's Objective and Scope of its Activity

The purpose of the committee is to provide recommendations both for the FCC and for the telecommunications industry that, when implemented, will assure optimal reliability and interoperability of, and accessibility and interconnectivity to, the public telecommunications networks. The committee will address:

1. Barriers to Interconnectivity, Interoperability and Accessibility: The Committee will identify, and prepare recommendations to avoid, 1) barriers to the interconnectivity, interoperability and accessibility of public telecommunications networks and 2) barriers to the interconnectivity, interoperability and accessibility of telecommunications devices with those networks. The recommendations will ensure the ability of users and information providers to seamlessly and transparently transmit and receive information between and across telecommunications networks.

2. Oversight of Coordinated Public Telecommunications Network Planning and Design: The Committee will consider, and provide recommendations on, how the Commission most efficiently can conduct effective oversight of coordinated telecommunications network planning and design to assure optimal reliability, interoperability, accessibility and interconnectivity of public telecommunications networks.

3. Standards-setting Organizations: The Committee will consider, and provide recommendations on, how the Commission most efficiently can participate in the development by appropriate industry standards-setting organizations of public telecommunications network interconnectivity standards that promote access to (1) public telecommunications networks providing telecommunications service; (2) information services by subscribers of rural telephone companies; (3) network capabilities and services by individuals with disabilities.

4. National Network Reliability: The Committee will report on the reliability of public telecommunications network services in the United States.

The committee will assemble data and information and perform analyses in order to provide to the Federal Communications Commission and the industry the reports and recommendations mentioned herein.

C. Period of Time Necessary for the Committee to Carry Out its Purpose

The committee will require between twelve and eighteen months to carry out its purpose.

D. Official to Whom the Committee Reports

Chairman, Federal Communications Commission.

E. Agency Responsible for Providing Necessary Support

The Federal Communications Commission will provide the necessary support for the committee, including the facilities needed for the conduct of the meetings of the committee. Private sector members of the committee will serve without any government compensation, nor will they be entitled to travel expenses or per diem or subsistence allowances.

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

The duties of the committee will be to gather the data and information necessary to form reports and recommendations to the industry and to the FCC for assuring optimal network reliability within the parameters set forth in Section B., above.

G. Estimated Annual Operating Costs in Dollars and Staff Years

Estimated staff years that will be expended by the committee are 2 for the FCC staff and 12 for private sector and other governmental representatives. The estimated annual cost to the FCC of operating the committee is $100,000.

H. Estimated Number and Frequency of Committee Meetings

The Council will meet at least semi-annually with possible more frequent meetings of informal subcommittees.

I. Committee's Termination Date

The Committee will terminate January 6, 1998.

J. Date Original Charter Filed

January 6, 1992

APPENDIX E

QUESTIONNAIRE RESPONSES IDENTIFY BARRIERS

Competitive and Sensitive Information

- Privileged Information Exchange: Effectively planning for interoperability will require the exchange of information between interconnecting companies which, in many instances, will require the revealing of market and strategic information. It is not clear how this information can be safeguarded while at the same time being responsive to the request.
- "Proprietary data" may be over-restrictive
- There is currently no industry clearinghouse that can coordinate access issues such as outside plant availability. Each provider plans services in a proprietary vacuum which stifles competitive entry and is both time consuming and costly. There needs to be a reasonable balance between strategic asset protection and strategic asset sharing. As it relates to facility access, the prevailing attitude seems to be those that have "it" don't want to share "it" and those that need "it" can't get "it".
- The foundation of the historic process has been the fact that interoperability has been an objective of network planning, so that all parties shared network planning information. In the past, the participants in the process has non-overlapping franchises, and the introduction of a new service capability required that all participants prepare in synchronism. In the future, some participants may consider such network planning information as competitive advantage, more important than the need for interoperability.
- Service differentiation and the need to be the first to "market" promotes "unique" solutions that often are near-term obstacles to interoperability.
- There is a trend in some industries to develop proprietary software and hardware which is not compatible with existing or emerging technology which locks in customers but locks out competitors. If this approach emerges in the telecommunications network industry it will fractionalize the networks, stifle competition and create greater consumer angst.
- Joint Planning Limitations
    - Unwillingness to share forecasts and planning information considered to be sensitive or proprietary in nature
    - Increased concerns over sharing information considered to be sensitive or proprietary with increased competition and expanded lists of service offerings
- Intense vendor competition
- Uncontrollable competition
- Vendor need for product differentiation
- From a wireless to wireless perspective, one of the current barriers to interoperability that we recognize stems from proprietary implementation of emerging industry standards. These implementation strategies lead to incongruities in interoperation and interworking. Part of the cause of this problem is the result of increased competition - the carriers want new features, while the manufacturers want to differentiate their products. I expect to see the

increasingly competitive wireless marketplace have even a greater impact on standards development and implementation.

- Mutual concerns of interconnecting service providers regarding access to customer proprietary or company competitive information or access to value added proprietary software.

Forecasts and Joint Planning

- Forecasts: For capacity planning to be cost effective and expedient, a process will need to be developed which will guide the development and agreement on forecasts, including period, termination/adjustment liabilities, *etc.*
- Network design plans timed to avoid network blockage
- Need for joint planning or standards associated with interconnection of local exchange carriers via shared two-way trunking (as described in the FCC's Order on local competition), including rules to define how traffic will be recorded and billed and rules defining overall accountability and dispute resolution.
- Deployment Timing and Budgets: Each company wanting to interconnect with another company will have a time line and schedule for deployment which best fits their market strategy and budget. This time line and schedule may not be compatible between companies. Moreover, if one company must build plant to accommodate the plans of another, the potential exists for the diversion of funds from the building company's plans to those of the requesting company. This is an untenable situation and guidelines will have to be developed to properly deal with it. This situation becomes even more difficult if multiple requests are made of the building company.
- AIN trigger points
- Probably the greatest threat to interoperability is the LECs' delaying electronic bonding with competitors. Experience so far is that the exchange of information (all types) with the LECs is un-mechanized, error-prone, expensive and slow. Presently we are exchanging information with LEC's manually (by 12 page fax in one case).The industry needs a single national standard, developed very quickly and governed by a national industry group.
- Incumbents have expected new entrants to conform to their procedures as opposed to working with the new entrants or even finding middle ground. An example was a LEC’s insistence on their control of the GNE.
- Need to derive methods of interaction that consolidate interface points and utilize information technology innovations.
- Joint planning limitations
    - Different planning and budgeting processes
    - Different perceptions as to how the network should be opened and unbundled for use by other service providers
    - Lack of common forums or activities involving all industry parties
    - Concern that such planning may be considered “collusion” or perceived as a violation of anti-trust laws
    - Continuation of present barriers
    - Different strategic plans for evolving the network
    - Different plans for new service offerings

    - Increasing number of participants (service providers, vendors, *etc.*) making it even more difficult to involve all industry parties
- Converging network technologies with the use of multiple access technologies.
- In short, Focus Group 1 should address issues on how to streamline processes to maximize utilization of the telecommunications network; reduce the time required to enable effective interconnections and, minimize the costs required for effective interconnections.
- Technical impact of untraditional calling patterns/hold times (*e.g.*, Internet)
- Rapid rate of technology change
- Need for a well defined plan/schedule for implementation

Future Network Architectures

- Interworking of IP and ATM based networks: routing, numbering/addressing, *etc.*
- Interworking of private and public data networks, principally ATM.
- Interworking of network management (TMN) networks.
- Need to address ATM interworking issues including 1) narrowband PSTN with ATM broadband networks, (2) public and private ATM network interworking, and (3) ATM-based and IP-based network interworking including routing and addressing.
- Interworking of private and public data networks, principally ATM.

Interoperability

- The first is the entrance of new service providers and networks into the marketplace. Simply by the entrance of so many new Telecommunications Service Providers, the complexity of interconnection is increased.
- Too few interconnection points
- Ability of carriers to manage the evolution of their networks in an interconnected environment. For example, if an area is presently served by copper, and unbundled loops are used for ADSL/HDSL, how can the feeder route be converted to digital loop carrier?
- The complete deployment of fully distributed systems will stress interoperability to the maximum “thruput & functionality”
- Too many levels of potential interoperability (software, hardware, ops, *etc.*)
- Network accessibility implies that operators of competing or interconnecting networks require access to each other’s networks on a basis that would allow for timely interconnection and effective interworking. This is an issue for the first sub-group, and will be addressed following:

  It is obvious that the new participants in the industry will have a very different spin on this issue than will telecommunications services providers designated as “Incumbent LECs “. Their impressions could well serve as a beginning point of discussion. But at the beginning, an overall principle that should apply to this discourse is that parties should be obligated to support the activities of others only to the extent that interfaces and functions are defined in accordance with industry rules and agreements, but that each network should stand on its own.

  In order to be effective in establishing which service structures are to be transparent across networks, I believe the group should address the issue of what are and what are not

national services. A perfect example is 800 service; all LECs will have to provide this capability. An example of a service that can appear across networks, and probably should, is CNAM. In order to go about this effectively, I believe that we must reach some philosophical understanding as to what services are national and must be transparent, and those in which the various carriers have the opportunity but not the obligation to cooperate so that services appear seamlessly across networks. An example of one that could go either way and is yet unresolved is 500 service.

My view as of now is that a significant barrier is lack of common understanding on what these boundaries are.

- Lost responsibility for infrastructure (software defined systems)
- An issue which has potential to inhibit interoperability is the one of tandeming. It will not make economic sense for us to have direct trunk groups to every LEC and IXC. So, it is critical that either the LEC or third party provider provide economical tandeming functionality.
- Harmonization of the growing IP-based packet networks with today's TDM-based circuit switched networks for service optimization.
- Market forces drive to inferior technology (Betamax syndrome)
- Extensive distributed hardware and networks
- Service providers willingness to accept "local" solutions
- Large variety of networks

Management/Operational Interfaces

- Changing Technology - As new networks are introduced, for example, ATM networks, the number of interoperability interfaces will continue to increase, making interoperability more complex and costly.
- Certain forms of interconnection such as mid-span or mid-air meets will greatly increase the number and types of network interfaces and require the installation and maintenance of a myriad of equipment configurations, brands and vintages.
- Broadband deployments will require entirely new networks that will have to be interfaced with the public switched network and Internet
- PSTN

  I have also looked into problems that manufacturers appear to be having with new PSTN CLASS services, particularly Caller ID (number and name) and Call Waiting ID (number and name). I understand that some manufacturers have experienced problems in getting CID-Name from some switches - I am working on the details. I have also been told by Colonial Data Technologies (a manufacturer of CID and CWID display equipment) that within NYNEX some parts of our network in which concentrators have been used appear to be causing problems in getting CID-Name details - I am waiting for more details.
- Physical and logical access to incumbent network service elements
  - Switching
  - Directory/Operator Services
  - Common Channel Signaling (CLASS features/services, *etc.*)
  - Service Control Points (LIDB, *etc.*)

- Network to network interface standards for reliable transport of services containing multiple protocols across heterogeneous networks

Numbering, Addressing & Dialing

- National and international numbering plan for data addresses
- Delayed implementation of final number portability. Every day of delay prevents network interoperability and costs new entrants money and customers.
- Local number portability
- Limited Number Portability - The number that identifies a customer in today's networks is generally owned by the telecommunications administration, not the customer. This limits the movement of customers across networks.
- Number Portability between systems
- Universal dialing plan
- Expanded CIC codes and ability to combine multiCIC traffic on common access groups
- Integrated Access Networks - The access networks (network termination interface to central office) that are available to the public today are integrated into one administration's overall telecommunications network. These access networks do not allow for "dial-tone" to be easily offered by competing administrations
- Expanded use of information digits and standardized implementation
- Location portability in multi-network environments
- Number portability between service providers
- Addressing in multi-network environments
  - PINs
  - Telephone Numbers
  - IP addresses
- Service(s) portability in multi-network environments
- Universal accessibility to services and features

Operations Systems

- Security and reliability of customer and network provider data with interconnection of operations support systems.
- Support System Standards: Industry standards do not exist in many cases for the support systems (OAM&P) associated with some of the newer and existing network element (NE) technologies. The support systems which are available are generally vendor proprietary. This will impact the ability of the interconnecting companies to support interoperating technologies unless the companies purchase their equipment and associated support systems from the same vendor. This becomes increasingly complicated as the number of companies wanting to interconnect with one another grows. In addition there are virtually no support system-to-support system standards today. Even if the same vendor's equipment is purchased, interoperating companies cannot conveniently communicate between each others support systems.
- Lack of appropriate gateway interfaces to partition access to LEC Operations Systems data while safeguarding customer proprietary network information.

- Legacy Support - As new networks are introduced, there will be a temptation to discontinue support for older access mechanisms. This may marginalize elements of the population that cannot afford to replace their existing equipment.
- Joint planning limitations
    - Different operations objectives and strategies
    - Different mechanized planning tools
    - Different operations plans and systems

Performance and Measurements

- No single entity responsible for performance
- Access to unbundled service statistics and operational measurements for switching and transmission technologies
- Global Service Requirements - Services such as voice transmission require that certain parameters, for example delay and jitter, be allocated across all networks that the service crosses. The more liberal the interconnection of networks, the more difficult it will be to specify and meet the global parameters.
- Need to avoid or eliminate differences in network management protocols (*e.g.,* SNMP vs. CMIP) and information models used by interconnecting networks.
- Recovery and Analysis - Tracking and fixing problems across multiple interconnected networks is difficult and will become more so as more combinations of networks from different administrations becomes possible.
- Increased potential for "chain reaction" outages (co-dependency)
- Drift to lower performance standards
- Lack of accountability in incidents that jeopardize network reliability or performance.
- Distributed responsibility for customer service
- RBOC/LEC maintenance of any databases that impact competitors, even something as "public spirited" as maintaining the E911 database.
- Network Management:
    - OAM&P Procedures
    - Alarms/trouble call resolution
    - Escalation Procedures
    - Installation Services
    - QoS Performance Standards

  Network management across multi-network environments
- Disaster recovery and survivability in multi-network environments
- Appropriate process and business agreements for dealing with reliability issues. *i.e.,* natural disasters, *etc.*

Processes

- Need for development of consistent information models for electronic interfaces to Support ordering (NC, NCI codes, product definition) of local exchange services.
- Standardization of order entry, tracking and service interfaces

- A second potential future barrier may be an inability to prioritize desired features and points of access. For any potential capability there needs to be a sufficient market to justify the cost.
- Incumbents should not be allowed to dictate the terms of installation for facilities-based competitors. For instance, when a competitor installs service, that competitor has the right to access the inside wire. If the Incumbent has not installed the appropriate inside wire interface, they have no right to delay the competitor while they process paper or dispatch people to disconnect their network from the inside wire.
- With respect to industry procedures, what process should be developed that enables industry to agree upon procedures that effectively address interoperability while minimizing the amount of development resources that would be required for the implementation of the procedures?
- Lack of standardized approach for service provider and/or billing provider identification in a local competition environment
- How can current industry processes be enhanced to maximize participation by new entrants into the telecommunications industry and accommodate the broadest array of end users using the widest variety of customer-provided equipment?

Security

- Lack of efficient, secure electronic interfaces to share network reliability data, orders and troubles.
- Security: Effective interoperability will require the exchange of signaling, control and maintenance information across interoperating interfaces. This information can have a major and catastrophic impact on the network of an interconnecting partner if sufficient safeguards (*e.g.*, firewalls, message screens, *etc.*) are not in place. Currently, most technologies, particularly access technologies, do not have these types of safeguards in place.
- Increased scam opportunities (pay phone slamming, wireless cloning, *etc.*)
- Service security in multi-network environments

Signaling

- Lack of consistent synchronization plans and technology will affect interoperability
- Lack of consistent synchronization plans and deployment are limiting interoperability
- Need for interoperability of common channel signaling systems including the ability to collect utilization data at the carrier level for a large number of carriers, and to transmit the data for billing purposes.
- Security, reliability and service quality (*e.g.*, in the face of uncontrolled traffic) in interconnected signaling networks (SS-7, database, AIN).

Terminal Equipment, Internet, Private Networks

- Need for well-defined and documented interfaces for new equipment and interconnection points associated with expanded interconnection requirements.
- Need for points of interconnection and collocation to conform with minimum standards of the technical feasibility definition regarding network evolution.

- Proprietary protocols from network equipment manufacturers are current barriers to interoperability between network elements and between networks.
- The integration of Internet has a large number of unknown interoperability problems
- Extension of direct ATM interfaces to CPE in a standard fashion to realize multimedia applications.

Testing Interconnecting Networks

- Need for interoperability testing for interconnecting networks (*e.g.,* SS-7 interconnection) and equipment which have not been tested.
- No single entity/standard for interconnection testing
- Adequate test plans among multiple players to avoid diagnosis and fix delays
- Inadequate testing due to rapid development of new technologies:
  Lack of uniform testing procedures;
  No clearly-articulated telecom disaster response and recovery procedures
- Resources, cost (funding mechanisms and cost recovery) and time required for interoperability testing for interconnecting networks (*e.g.,* SS-7 interconnection).
- Lack of national commitment to true interoperability testing
- Lack of efficient, automated test access to unbundled/interconnected loops.
- National commitments to broad interoperability testing
- Additional concerns include security, partitioning and operational/administrative issues, such as access to monitoring information, testing, *etc.*
- Untested technologies being implemented too fast
- Adequate testing

Vendor Compatibility/Standards

- Equipment compatibility between vendors is still not good at high speeds (OC12, OC48), *i.e.*, AT&T OC-12 won't work well (or in some cases at all) with a Fujitsu or NEC multiplexer, so when LECs dictate the equipment vendor, it causes compatibility problems. CPE equipment is generally much better at interoperability than network equipment, but even some ISDN phones won't work with all switches
- Vendor Product Incompatibility: Vendors at time have differing interpretations of industry standards which inhibit/prohibit the interworking of their equipment.
- Joint planning limitations
  - Use of products and equipment from different suppliers
- Standards implementation requires interpretation of gray areas
- Another cause of interoperability problems results from manufacturers interpreting and implementing industry standards differently
- Need for a common understanding/definition of a service/interconnection arrangement
- Need for national mandatory minimum standard set

Standards (forwarded to Focus Group 2)

- With respect to standards/requirements, what is the minimum set that needs to be met to ensure interoperability?

- No agreement on protocol “TCP/IP vs. OSI/CMISE”
- Need for well-defined and documented interfaces for new equipment and interconnection points associated with expanded interconnection requirements.
- Lack of efficient, secure electronic interfaces to share network reliability data, orders and troubles.
- Increased need for information requirements and formats due to rapidly increasing number of service providers with wide variation in type, size, level of sophistication, and performance standards.
- Lack of appropriate gateway interfaces to partition access to LEC Operations Systems data while safeguarding customer proprietary network information.
- Need for points of interconnection and collocation to conform with minimum standards of the technical feasibility definition regarding network evolution.
- From a pure wireless to wireless perspective, one of the current barriers to interoperability that we recognize stems from proprietary implementation of emerging industry standards. These implementation strategies lead to incongruities in interoperation and interworking. Part of the cause of this problem is the result of increased competition - the carriers want new features, while the manufacturers want to differentiate their products. I expect to see the increasingly competitive wireless marketplace have even a greater impact on standards development and implementation.
- The comments which follow focus on barriers to effective and efficient network-to network interoperability from the perspective of capacity and implementation planning. Architectural issues are principally the domain of industry standards bodies and, as such, it is assumed that Focus Group 2 will be addressing these Issues. In addition, at this stage of analysis, it is difficult to differentiate between near term and long term barriers. Therefore, the thoughts which follow are not differentiated by time, but are offered as barriers in general to efficient and effective interoperability.
- Support System Standards: Industry standards do not exist in many cases for the support systems (OAM&P) associated with some of the newer and existing network element (NE) technologies. The support systems which are available are generally vendor proprietary. This will impact the ability of the interconnecting companies to support interoperating technologies unless the companies purchase their equipment and associated support systems from the same vendor. This becomes increasingly complicated as the number of companies wanting to interconnect with one another grows. In addition there are virtually no support system-to-support system standards today. Even if the same vendor's equipment is purchased, interoperating companies cannot conveniently communicate between each others support systems.
- Network overhead standards for SONET systems supporting provisioning, administration and restoration
- Standardization of order entry, tracking and service interfaces
- Expanded use of information digits and standardized implementation
- Global Service Requirements - Services such as voice transmission require that certain parameters, for example delay and jitter, be allocated across all networks that the service crosses. The more liberal the interconnection of networks, the more difficult it will be to specify and meet the global parameters.

- For wireless telephone systems, a barrier to interoperability is the lack of a standardized interface between the switch and base station transmitter. If such an interface were standardized, new wireless services could be more universally available to all Americans as infrastructure cost would be lowered through competition. Motorola therefore recommends that an industry standards body such as TIA develop a standardized switch to base transmitter interface.
- Standards process too slow
- Varying facility standards for PSN, cable, wireless systems
- Inconsistent performance standards/expectations for PSN, cable, wireless
- Proprietary protocols from network equipment manufacturers are current barriers to interoperability between network elements and between networks.
- Your initial questions were general in nature, but extremely important. As you can see by my response, a major focus regarding interoperability continues to be in the area of the development, agreement and implementation of standards. I expect, as we move forward, to get into some more detailed issues, especially those which may have been created by the recent FCC Order. Some which come immediately to mind include SONET interconnection, access to the AIN service creation environment, and customized routing for Switches and STPs.
- Standards bodies have historically been the basis for the development of the standards which facilitate interoperability. While standards for existing DSO, DS1 and DS3 interconnection are well defined, standards for emerging technologies such as SONET and ATM are not. These standards must be defined, agreed upon, and more importantly, implemented by the vendor community such that seamless interconnection and interoperability can occur. In many cases this must be done not only at the physical and electrical level, but also at the application/logical level where the interconnection takes place.
- Nonuniform implementation of the ISDN BRI standard deployed across the COs of the PSTN.
- Inability of the PSTN to support even the current V.34 standard data communications standard much of the time.
- This response takes into account the fax from Jim Keegan of 8/6/96 as
- well as that from Mr. Gunter first received here the week of 8/26.
  "What are the barriers to network accessibility and interconnectivity and what should be done to overcome those barriers"? (This from Keegan's earlier memo) First point is clarification - what is meant by "accessibility"? Service accessibility would indicate the ability of telecommunications users to provide the inputs necessary and receive the outputs in such a manner so as to be able to utilize network services. This would get into network interfaces to terminal equipment, and access by the handicapped to terminal equipment which includes many human factor issues, and in my view, should be addressed in the second sub-group.
- Standards development keeping pace with technical development
- A second potential future barrier may be an inability to prioritize desired features and points of access. For any potential capability there needs to be a sufficient market to justify the cost.
- Need for efficient, secure interoperability standards for carrier interworking to exchange network management data, orders, and trouble reports. Current recommendations such as

TMN's "X" interface for use between TMN administrative areas and the ATM Forum's M3 interface that addresses carrier to carrier issues require much work before these interfaces can be used to solve the interoperability requirements.

- Need to avoid or eliminate differences in network management protocols (*e.g.,* SNMP vs. CMIP) and information models used by interconnecting networks.
- Need for consistent and/or conformant implementation (including implementation timing) of TMN "X" interface across interconnecting management networks.
- In addition to the continued impact of competition on standards development mentioned above, new telecommunications media (*e.g.,* CATV, satellite, PCS) will impact interoperability among all networks in the future. Couple these issues with the development and implementation of the Wireless Intelligent Network (WIN - the wireless version of AIN), the development of open wireless network interface standards, and the recent FCC requirement for number portability and the need for increased communications and cooperation among the various standards organizations becomes critical.
- Secondly, the unbundling of services in existing networks will generate new requirements for standards.
- Finally, the pace of growth and change of technologies and network configurations will require swift response from the standards organizations as well as mutual cooperation among carriers.
- A standardized interface between switch and base station transmitters could be even more important going forward as wireless systems can provide local loop options as well as mobile service.
- Predicting future barriers is a guess, at best. However, as technology continues to proceed at a breakneck pace, the issue of standards becomes even more critical, especially in light of the relative slowness of the standards process. Not only will technical interoperability (physical, electrical, logical) be an issue, but the future signaling and control of that network infrastructure will become increasingly complex and affected by more and more players. For instance, interoperability in the future may become more complicated should we transition to an AIN-like control of the Broadband network to provide bandwidth-on-demand, anywhere, anytime, across networks. Control and signaling related to Local Number Portability and PCS is also likely to present significant interoperability challenges. We also need to be cognizant of the increasing number of de facto standards which have occurred, especially in the computer and Internet industries, and how these de facto standards may impact telecommunications interoperability in the future.
- SONET standards should drive multi-vendor equipment compatibility in the future.

Not Technical

- Administration and Accounting - Charging for use of resources when multiple networks are used for a customer's service will need to be made easier and more flexible
- Overinvestment in competitive marketing vs. technology/infrastructure
- Unclear Government role/policy/requirement
- Untested legal/constitutional issues
- The biggest barrier of all is the unsettled situation in regard to obligations under the FCC's current rules. I anticipate that participants are going to be very cautious in not agreeing to

things here that have the effect of forfeiting any of their options in this process in regard to their statutory obligations. Until many of these issues are settled the various parties to this process are going to have to exhibit significant good will and sensitivity to determine what issues we can work and which have to wait until some specific requirements are better defined.

- It is not possible to really evaluate this one until we determine what the present barriers are and how we are to address them. In addressing current concerns, we need to continuously test the issues and outcomes to be sure that we are not somehow compromising future expectations as a result of current actions.
- Clearly, continued regulatory uncertainty could be a major future barrier.
- A second issue was addressed in Jim Keegan's memo - it is not clear whether you intended to address it at this time. But follows a brief "take" on it. "What procedures should the FCC follow to conduct effective oversight of network planning to assure optimal reliability, interoperability and accessibility of telecommunications networks"?
    - It is almost easier to first state what the FCC should not do. It should not establish itself as an engineering design bureau for telecommunications networks, and it should not become a technical standards developer. Current ANSI - accredited groups and their work should be recognized. The consensus forum process should also be reaffirmed as a preferred process.
    - In many cases, frustration has been expressed with the slowness of the process. But in many cases, it is the lack of response from the Commission itself that has been a problem. Commission staff has the opportunity to attend and observe meetings of industry groups and has done so in the past. I also believe that the Commission staff has been correct in not intervening in the process to influence the outcome on specific technical issues.
    - But Commission staff observers should be empowered to accept assignments for working within the Commission itself. In an industry activity, an issue often arises in which regulatory uncertainty creates a situation in which agreements cannot be reached. The forum should be able to determine that some regulatory action or determination is necessary in order to permit the process to continue in a productive manner. Such a determination should be able to be forwarded to the Commission for action and subsequent notification of the outcome so that the forum may proceed with its activities.
- This is in response to your request of August 14, 1996 for data to establish a work plan for Focus Group 1 of the FCC's Network Reliability and Interoperability Council (NRIC). As detailed below, we are concerned that your proposed approach of attempting to identify present and future "barriers" to interoperability may be setting the wrong tone for the work of Focus Group 1.
    - The Increased Interconnection Focus Group of NRC II basically concluded that existing industry processes will need to evolve to accommodate future interconnections, but that radical changes do not appear to be needed. We participated in this Focus Group and continue to support its conclusions. While there are currently many technical and operational issues that must be addressed to facilitate interoperability, we could not identify any that were not being worked and could be considered a current barrier.

Similarly, the future will undoubtedly be more complex with respect to interoperability because of such things as new technology and an expanded set of players. This will undoubtedly result in a new set of issues to be worked, but none should be construed as barriers. In short, the telecommunications industry has made significant progress in addressing interoperability issues. However, with the current emphasis of the Focus Group on barriers, this progress may be forgotten and the false impression given that serious unsolved interoperability problems exist that the telecommunications industry does not know how to solve.

- As alternative to the current approach, Focus Group 1 should review the work of the Increased Interconnection and Changing Technologies Focus Groups from NRC II and determine how their recommendations can be enhanced to address the current and future telecommunications environments.
- While this initial input does not follow your requested format, I trust it will, nonetheless help in the development of a work plan for the two subcommittees of Focus Group 1.

Other

- A number of issues are raised by this question depending on the perspective from which the question is being answered. Thus, it would seem very important in providing an answer to consider that perspective, by seeking the answer to such additional questions as listed below. The questions are derived by looking at the actual words of Section 256. These questions would also seem to suggest that input (perhaps as a response to a survey) from a broader group than those represented on this Focus Group could be an exercise which would produce some meaningful input.
- What is nondiscriminatory accessibility?
- Who are the telecommunications carriers and other providers of telecommunications services?
  - How do they promote nondiscriminatory accessibility of public telecommunications networks to other public telecommunications networks?
  - How do these carriers and other providers promote nondiscriminatory accessibility of public telecommunications networks by vendors to products (*i.e.*, equipment used by providers of network services within their networks) and of services (*i.e.*, communications services used by providers of network services)?
  - What are some specific examples of such barriers that exist today? Are they likely to be removed?
  - What examples are there of barriers to the accessibility of networks by providers of network equipment?
  - To what extent do public telecommunications networks permit other networks and network equipment to "seamlessly and transparently" transmit and receive information between telecommunications networks? Are there any barriers to the seamless and transparent transmission?
  - How is coordinated network planning and design among telecommunications carriers conducted today?

- Does coordinated network planning as it is done today assure nondiscriminatory accessibility? If yes, how? If it does not, how should it be conducted?
- Does the coordinated network planning and design assure the interconnection of the public telecommunications networks used to provide telecommunications services?
- These represent some of the questions which seem to flow from the Question I as it was initially raised as well as being questions which are raised by taking a closer look at the wording of Section 256. With regard to Question 2 as posed in the August 14, memorandum from you, it would seem that the same questions listed above could simply be asked in a future context to generate information in response to Question 2.

- We must not lose sight of our history. The telephone network has always been provided by multiple carriers, and the industry has evolved a comprehensive process for insuring interoperability. This process has focused on technical issues. A potential barrier that must be avoided is that we ignore this tradition and act as though interoperability among multiple carriers is a brand new issue created by the 1996 Telecommunications Act. The focus must remain on technical issues; policy issues should be dealt with in other, appropriate, forums.
- Considering the current environment, the interoperability among carriers is and has been successful. The success is based largely on the efforts of various industry associations such as the Committee T1, T1A, ATIS, NOF, *etc.* that have succeeded in defining standards. Additionally, industry cooperation among and between companies has driven interoperability in terms of network interfaces, both physical and logical, network performance and management processes, and network security. The work performed by the Network Reliability Council - Task Group II, provides direction defining the process and role of standard development. Some excellent output is offered by the group with the "Network Interconnection Bilateral Agreement Template" and "Network Interface Specification Template". In summary, this very competitive, fast-paced industry has taken the necessary measures through the support and participation of the standards organizations to ensure networks mesh into seamless interoperability in the best interest of the public.
- I have begun an inquiry into Network-CPE interoperability issues:

  ISDN

  I have not found instances where NI-1 equipment failed to operate on NI-2 circuits. Until recently, we were having an enormous problem getting the proper ISDN switch settings for different types of ISDN CPE. NYNEX has now, along with most other regions, settled on 5 standard ISDN switch configurations that we are requiring manufacturers to specify for their CPE. This seems to have made many of the CPE manufacturers unhappy, but my understanding is that it has greatly improved the probability of getting CPE to work right out of the box.

  All in all, I have not identified large scale Network-CPE interoperability problems with ISDN or PSTN. I will continue to consult with manufacturers. I have not yet begun an inquiry into faster circuits such as TI and frame relay or larger pieces of CPE such as PBX'S.

APPENDIX F

THE NETWORK RELIABILITY AND INTEROPERABILITY COUNCIL

Member Organizations (by primary identity)

Interexchange Carriers
AT&T
MCI
Sprint

Local Exchange Carriers
Ameritech
Bell Atlantic
BellSouth
GTE Corporation
NYNEX Corporation
Pacific Telesis
Southwestern Bell
US West, Inc.
Frontier Corp.

Research and Standards Organizations
Bell Communications Research
Alliance for Telecommunications Industry Solutions
Cable Labs
Telecommunications Industry Association

Internet Access Providers
America Online

Trade Associations
Association for Local Telecommunications Services
Competitive Telecommunications Association
Organization for the Protection and Advancement
of Small Telephone Companies
United States Telephone Association
National Cable Television Association
Cable Telecommunications Association
Personal Communications Industry Association
Cellular Telecommunications Industry Association

Institutional Consumer Representatives
Tele-Communications Association
International Communications Association
Boeing Company

Residential Consumer Representatives
Alliance for Public Technology
National Association of State Utility Consumer Advocates

Cable Companies
Time Warner Communications

PCS Representatives
NextWave Telecom, Inc.

Manufacturers
Motorola
U.S. Robotics
Lucent Technologies
Nortel

Government Related Organizations
National Association of Regulatory Utility Commissioners
National Communications System

Labor Representative
Communications Workers of America

Satellite Service Providers
Hughes Telecommunications and Space Company --
Hughes Electronics Corporation

Computer/IP Industry
Information Technology Industry Council (also representing
Information Infrastructure Standards Panel)

Associate Members
National Telecommunications and Information Administration,
U.S. Dept. of Commerce
Office of Science and Technology Policy, White House