NETWORK RELIABILITY AND INTEROPERABILITY COUNCIL VI

HOMELAND SECURITY
PUBLIC SAFETY
(FOCUS GROUP 1C)

FINAL REPORT

ISSUE 2, APRIL 2003

Table Of Contents

1 Executive Summary

The objectives of the Network Reliability and Interoperability Council VI (NRIC VI), Homeland Security Focus Group Public Safety Subcommittee (FG-1C) were 1) assess the level at which commercial communications services are currently used by the Public Safety community, 2) gather information on the perceived needs of the Public Safety community in terms of commercial communication services, 3) perform a gap analysis to identify opportunities where commercial networks can aid the Public Safety sector, and 4) present recommendations to address these opportunities.

Objectives

1) The FG-1C subcommittee's first task was to make an assessment as to what commercial applications are currently being used by the Public Safety Sector and identify which if any Best Practices existed that applied to those applications or services.

   In general, the Public Safety Sector relies on private radio network/services for many if not most of its communications needs. However, as the events of September 11th cruelly highlighted, during catastrophic events, the existing communication services faced substantial challenges. Coverage, inter-agency connectivity and general survivability were major issues that begged to be addressed.

   While FG-1C will not address the private networks themselves, it must be recognized that the private radio networks in use by the Public Safety Sector rely in no small measure on commercial communications carriers for their backbone infrastructure and/or transport between elements of a private network. In addition to their private radio networks, the Public Safety Sector relies on commercial paging services and of course commercial wireless offerings. The existing catalog of Best Practices (BPs) contains an extensive number of practices relating to just these types of services and architectures.

   These BPs covered issues including facilities and network design and operation, disaster recovery, emergency preparedness, security, interoperability, policy and essential services. Once existing BPs were identified, they were reviewed, applicability was assessed, and if necessary modifications were considered. These existing BPs covered the wireline, wireless, cable, satellite, paging and Internet segments of the industry.

2) At this point, FG-1C now had a general picture of how commercial communications were already supporting the Public Safety Sector and their private networks. It was now time to identify what the Public Safety community perceived as their needs. As a means to gather this information, FG-1C circulated a survey to members of the Public Safety community (See Appendix C for an example of the survey questionnaire). The intent of the survey was to gather information from individuals who are directly involved during a

"major response" such as one caused by a natural disaster, terrorist attack, or other catastrophic event.

In particular the survey requested information on:

Demographics

- Agency Information – public service agency with which they are affiliated
- Position & Responsibility – position within that agency and areas of responsibility
- Jurisdiction – Local through National

Usage

- Extent to which they use commercial networks.
- When and how they use commercial networks during a major response.

Familiarity with commercial emergency services

- GETS
- PAS

Wish List

- What services or capabilities would they like to see deployed

The survey was circulated initially at industry forums. Later, participants were asked to visit the NRIC website and follow a link to an electronic version of the survey. We received 229 responses. (For a hyper link to view the raw data gathered please see Appendix F.)

In addition to the survey responses, one on one interviews were conducted with participants of the survey who had graciously provided contact information.

3) Once the raw data from the survey had been compiled and summarized, a gap analysis was performed. The various commercial communications industry segments that had been the focus of the survey were addressed individually. These segments were wireline communications, wireless communications, cable communications, the Internet and satellite communications.

Across each segment, the needs as identified by the Public Safety community were compared to the existing BPs compiled during the initial assessments. As existing BPs were matched up with the needs of Public Safety, the BPs were validated and modified if necessary. When a Public Safety need was identified for which no current BP existed, the teams formulated a recommendation to deal with the shortfall.

4) The BPs and recommendations generated through the gap analysis process address a number of industry and network concerns. In general, survivability was of primary concern. BPs and recommendations dealing with architectures incorporating redundancy and diversity were a major focus along with the identification and inventory of critical circuits or infrastructure. Also of critical concern was the incorporation of priority of services during a crisis situation, restoration of critical services and emerging emergency services.

Best Practices have traditionally focused on telecommunications and communications carriers, and communication equipment vendors. In contrast, BPs and recommendations generated by FG-1C regarding Public Safety not only incorporate traditional communication issues, but incorporate issues of concern to Public Safety entities, Emergency Management Services, Municipalities and Private Sector players. As such, a more extensive outreach program for the dissemination of the information contained in the BPs and NRIC recommendations will be necessary.

As the Focus Group analyzed Best Practices in the context of the range of services and how these services relate to public safety's myriad circumstances, it comprehended that rarely do changes take place without impacting resources. While it is possible that a revised or new Best Practice or recommendation can reflect a more efficient and effective method, thereby limiting cost implications, the more likely circumstances is that there will be a cost involved. This is particularly true in this initiative exploring the public safety sector where the goal is improving access, redundancy and reliability of not one but all the available services. The Focus Group recognized that parallel to providing tangible assistance to public safety's commercial communications services through changes in Best Practices, it is of equal importance that resources are made available to pay for the changes, resources that ultimately have to be paid for by the customer, usually the government agency acquiring the service or equipment. The Focus Group acknowledges that change and the availability of resources are not separate issues, but are inextricably tied.

The Best Practices, while not industry requirements or standards, are highly recommended for implementation. As The First Council stated, “Not every recommendation will be appropriate for every company in every circumstance, but taken as a whole, the Council expects that these findings and recommendations [when implemented] will sustain and continuously improve network reliability.” This statement can now be extended to include Public Safety. NRIC Best Practices result from broad industry cooperation that engages vast expertise and considerable voluntary resources. Efforts by government authorities, to impose these as regulations, may jeopardize the industry’s willingness to work together to provide such guidance in the future.

Detailed information on the abstracted information included in the Executive Summary is provided in the relevant report sections and appendices.

2 Introduction

The Public Safety Focus Group is the third of four sub-groups that collectively form the new Homeland Security Focus Group for NRIC VI. The Physical Security, Cyber Security and Disaster Recovery Focus Groups represent the additional three priorities established by the Sixth Council to address security in the Homeland. The Council has also added Broadband Reliability as a new Focus Group in addition to continuing the work of previous Councils on Network Interoperability and Network Reliability.

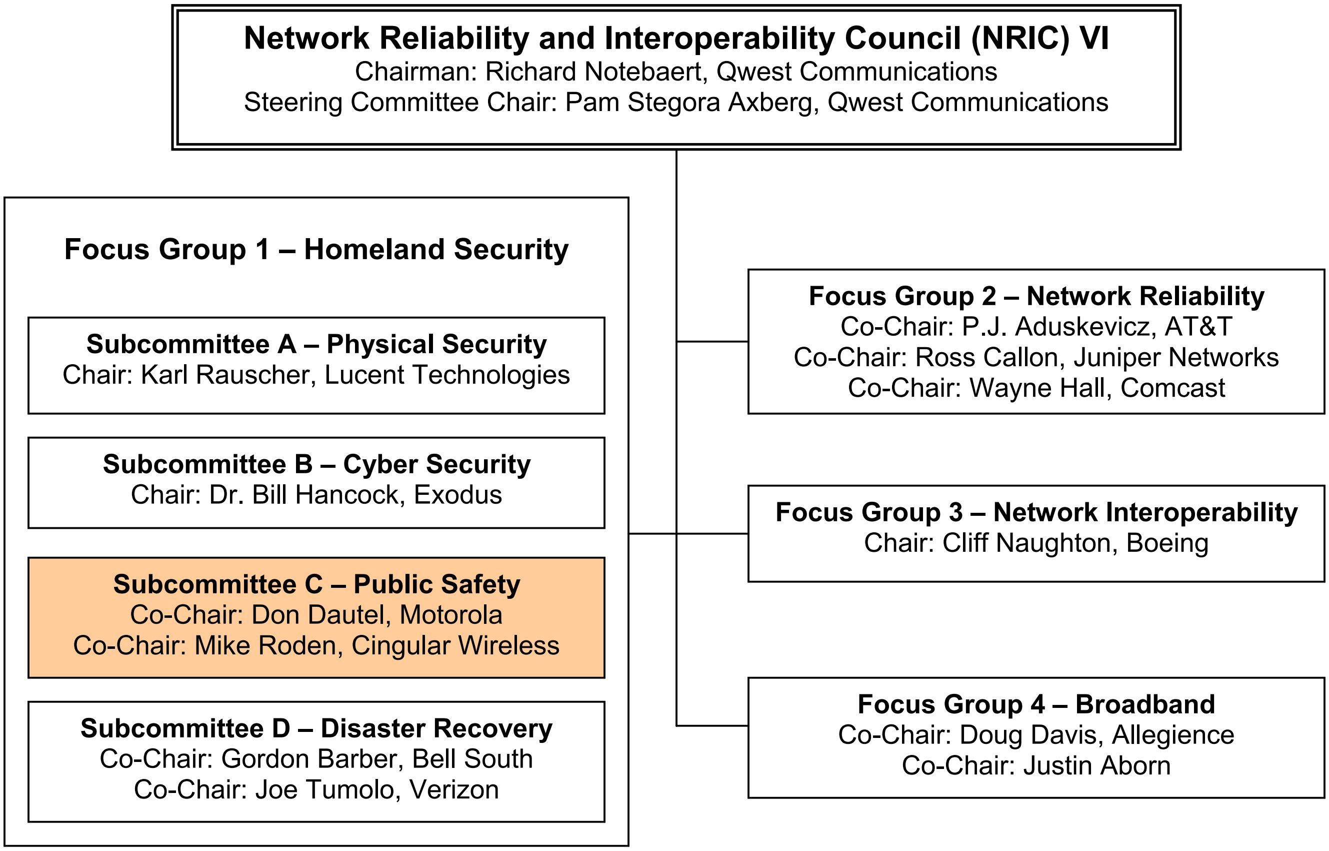
The FG-1C Committee is comprised of volunteers who represent LECs, ILECs, CLECs, Wireless Carriers, Cable Industry experts, Satellite Industry Experts, Equipment Vendors, the Alliance for Telecommunications Industry Solutions ("ATIS") and Telcordia. In addition members from the Public Safety Sector are represented. They include the International Association of Public-Safety Communication Officials-International ("APCO"), National Emergency Number Association ("NENA") members, and the National Communications System (NCS). We thank everyone for sharing his or her time, talents and expertise.

2.1 Mission and Structure of the NRIC VI

The purpose of NRIC VI is to give communications industry leaders the opportunity to provide recommendations to the FCC and to the industry in general that, if implemented, would under all reasonably foreseeable circumstances assure optimal reliability and interoperability of wireless, wireline, satellite, paging, Internet and cable public communications networks. This includes facilitating the reliability, robustness, security, and interoperability of public communications networks.

The scope encompasses recommendations that would ensure the security and sustainability of public communications networks throughout the United States; ensure the availability of adequate public communications capacity during events or periods of exceptional stress due to natural disaster, terrorist attacks or similar occurrences; and facilitating the rapid restoration of communications services in the event of widespread or major disruptions in the provision of communications services.

NRIC VI is structured as follows:



Network Reliability and Interoperability Council (NRIC) VI
Chairman: Richard Notebaert, Qwest Communications
Steering Committee Chair: Pam Stegora Axberg, Qwest Communications

Focus Group 1 – Homeland Security

Subcommittee A – Physical Security
Chair: Karl Rauscher, Lucent Technologies

Subcommittee B – Cyber Security
Chair: Dr. Bill Hancock, Exodus

Subcommittee C – Public Safety
Co-Chair: Don Dautel, Motorola
Co-Chair: Mike Roden, Cingular Wireless

Subcommittee D – Disaster Recovery
Co-Chair: Gordon Barber, Bell South
Co-Chair: Joe Tumolo, Verizon

Focus Group 2 – Network Reliability
Co-Chair: P.J. Aduskevicz, AT&T
Co-Chair: Ross Callon, Juniper Networks
Co-Chair: Wayne Hall, Comcast

Focus Group 3 – Network Interoperability
Chair: Cliff Naughton, Boeing

Focus Group 4 – Broadband
Co-Chair: Doug Davis, Allegience
Co-Chair: Justin Aborn

2.2 Focus Group Charter and Mission

2.2.1 Charter

The Committee will explore and report on such actions as may be necessary or desirable to ensure that commercial telecommunications services networks (including wireless, wireline, satellite, and cable public telecommunications networks) can meet the special needs of public safety emergency communications, including means to prioritize, as appropriate, public safety usage of commercial services during emergencies.

2.2.2 Mission

Focus Group 1C will conduct an assessment of the commercial communications service needs of the Public Safety community in times of crisis. The Focus Group will then perform a gap analysis to determine shortfalls, and will make recommendations to address these issues.

2.3 Focus Group Scope

2.3.1 Public Safety

The term *Public Safety*, as defined by the PSWAC (Public Safety Wireless Advisory Committee) report, extends to all applicable functions at the federal, state and local levels, including Public Safety operations on Department of Defense facilities. The PSWAC report identifies two levels of Public Safety providers, *Public Safety Service Provider* and *Public Safety Support Provider*. The Public Safety Services Provider is defined as entities performing such duties as emergency first response and similar activities. The Public Safety Support Provider is defined as entities whose primary mission may provide vital support to the general public and/or the Public Safety Service Provider. In the context of Homeland Security Public Safety Focus Group work, Public Safety includes both levels as listed below:

- Local, County, State and Federal Law Enforcement
- Local and County Fire Departments
- Emergency Medical Services
- Federal, State and Local Office of Emergency Management
- Communications Officers
- State and Local Government Officials

2.3.2 Network Types

The scope encompasses all sectors of the public communications infrastructure and includes all commercial communications networks, wireline, wireless, satellite, cable, and the Internet.

2.3.3 Industry Roles

The scope includes Service Providers, Network Operators and Equipment Suppliers of the public communications infrastructure, along with industry representatives (i.e. ATIS, NENA and Telcordia).

<u>Service Providers</u>

A Service Provider is an organization that provides services for end user customers, content providers and for users of a computer network. The services may include access to the computer network, content hosting, server of a private message handling system, news server, etc. A company, organization, administration, business, etc., that sells, administers, maintains, charges for, etc., the service. The service provider may or may not be the provider of the network.

<u>Network Operators</u>

A Network Operator is responsible for the development, provisioning and maintenance of real-time networking services and for operating the corresponding networks.

Equipment Suppliers

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

2.3.4 Public Safety Use of Commercial Infrastructure

Public Safety's requirement of commercial communications networks embraces three general aspects.

Reliability of Services

Public Safety private communication systems directly depend on the reliability/survivability of dedicated facilities that are obtained from commercial carriers and used as backbone infrastructure and/or transport between private network elements

Capacity of Networks

At another level, Public Safety has made increasing use of commercial communications networks for tactical support to supplement their mission critical private networks.

Emergency Telecommunication Services

At still another level, Public Safety can invoke the use of specialized emergency telecommunications services, such as priority access and emergency conference bridges, in times of crisis.

2.3.5 Focus Group Structure

The Public Safety Focus Group (FG-1C) includes in its membership, representatives from Public Safety Organizations as well as Manufacturers, Operators and Service Providers. The Focus Group participants are listed below in section 2.4. Due to the broad scope of this undertaking and the reduced deliverable timeframe, three subcommittees Wireline, Wireless and Cable/Internet were formed to efficiently analyze the data and report findings. Reeta Singh of AT&T Wireless followed by Tomas Bern of Ericsson led the wireless subcommittee. Lance Thomas of SBC followed by Dale Morgenstern of AT&T and Doug Jones of Verizon led the wireline subcommittee. Dan Sanders of Comcast lead the cable and Internet subcommittee.

The scope of the subcommittees' efforts included the commercial communications specific to the infrastructure and networks represented by the subcommittee and utilized by the Public Safety community.

2.4 Industry Participation

Due to the urgency and vital nature of its mission, the FG-1C set an aggressive schedule. 22 meetings were held between April 2002 and February 2003 that included over 2,200 participant hours. In addition, over 30 special Subcommittee meetings were held that included approximately 500 participant hours. The following organizations actively participated in the process:

- APCO
- BellSouth
- FCC
- Lucent Technologies
- Nextel
- Telcordia Technologies
- AT&T
- Cingular Wireless
- Hughes Network Systems
- Motorola
- Qwest
- VeriSign
- AT&T Wireless
- Comcast Cable
- Intrado
- NCS
- SBC
- Verizon
- ATIS
- Ericsson
- iXP
- NENA
- Sprint
- MCI

Also, additional expertise was engaged from other organizations when needed (e.g., International Association of Chiefs of Police (IACP), International Association of Fire Chiefs (IAFC), Public Safety National Coordination Committee (NCC), National Public Safety Telecommunications Committee (NPSTC), Public Safety Wireless Network (PSWN)).

2.5 Report Deliverables

The Homeland Security Public Safety Report, which is scheduled to be publicly available in March 2003, includes the following subject matter:

- Homeland Security Public Safety Mission, Scope and Approach
- Public Safety Survey Overview
- Participants
- Methodology
- Results
- Key Findings and Recommendations
  - ♦ Wireline
  - ♦ Wireless
  - ♦ Satellite
  - ♦ Paging
  - ♦ Cable
  - ♦ Internet
- Conclusions

To improve access to Best Practices throughout the industry, FG-1C plans to make the Best Practices available in a Web-accessible format that will include keyword search capabilities. The Focus Group will also provide information such as references, as appropriate, for individual Best Practices.

3 Public Safety Survey

The Focus Group decided that, in addition to the Public Safety representation, there was a need to reach out to a broad nationwide cross section of Public Safety agencies in order to obtain representative usage and requirement information. After reviewing several alternatives, FG-1C determined that a Web based survey would be the best approach. This decision was based on several factors including, time constraints, broad reach and cost effectiveness. A text copy of the survey is included in Appendix C.

3.1 Target Audience

The survey was oriented toward personnel of Public Safety agencies with emphasis on the First Responders to crisis situations and included representation from the following Public Safety agencies:

- State, County, Local and Federal Law Enforcement
- County and Local Fire Departments
- Emergency Medical Services
- Federal, State and Local Office of Emergency Management
- Communications Officers
- State and Local Government Officials

In addition to obtaining a broad cross section of Public Safety agencies listed above, the intent was to also obtain responses from a broad geographic and jurisdictional constituency.

3.2 Methodology

A web-based survey was chosen as the best method to meet the objectives within the time constraints established by the urgency of securing the Homeland. The survey was hosted on the NRIC web page under the Public Safety Focus Group section. It should be noted that the survey was intended to be qualitative in nature and therefore was not intended to be subject to quantitative statistical analysis. A number of efforts were undertaken to make Public Safety agency individuals aware of the survey and encourage their participation. Individual Focus Group members contacted various Public Safety Industry Associations as these were viewed as key channels of communication. Industry Associations involved in spreading awareness of the web-based survey include the following:

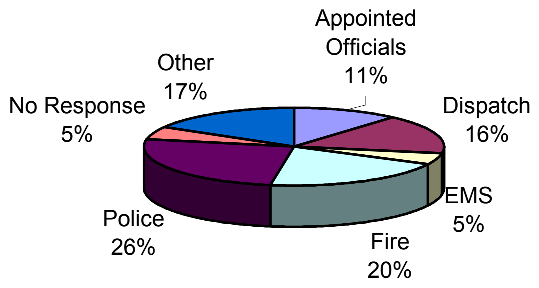
- Association of Public-Safety Communications Officials-International (APCO)
- International Association of Chiefs of Police (IACP)
- International Association of Fire Chiefs (IAFC)
- Motorola Telecommunications Users Group (MTUG)
- Motorola Data Users Group (MDUG)
- National Communications Council (NCC)
- National Emergency Number Association (NENA)
- National Public Safety Telecommunications Council (NPSTC)
- Public Safety Wireless Network (PSWN)

3.3 Data Analysis

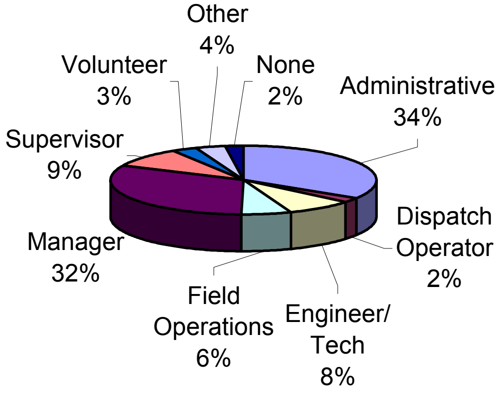
3.3.1 Demographic Information

In order to fulfill the objective of determining Public Safety's commercial communication needs, the Focus Group desired to obtain data from a broad representation of Public Safety agencies, agency size, positions, jurisdictions, roles and experience. To this end, the survey was successful; eliciting 229 responses from a broad variety of entities across the US and Canada. The following charts represent the demographic data of the survey respondents.

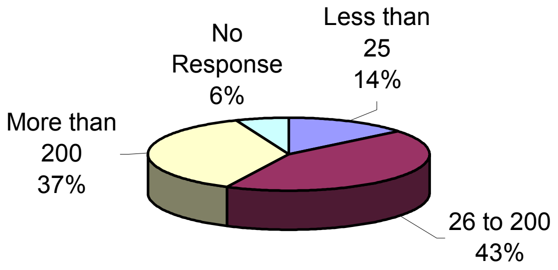
Responsibility



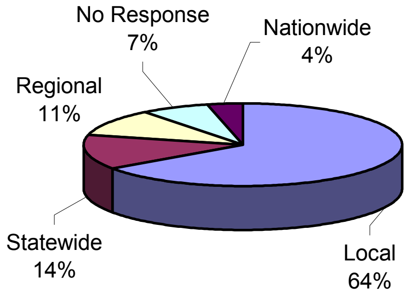
Position



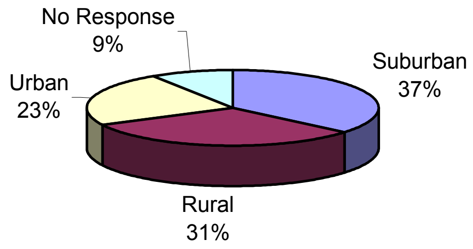
Agency Size



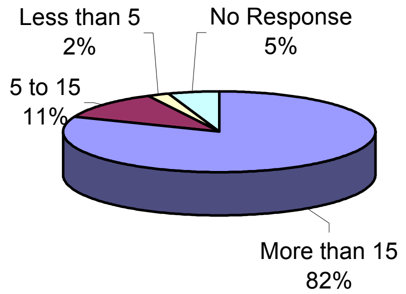
Jurisdiction

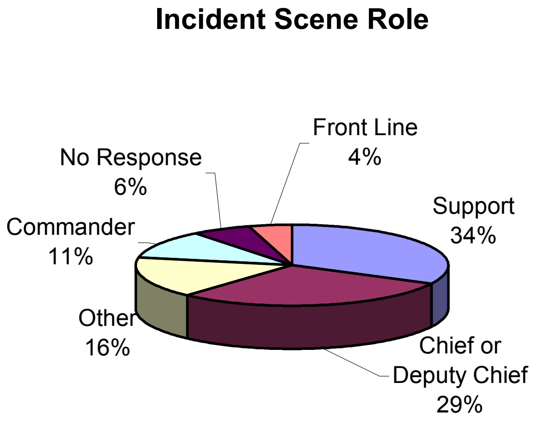


Jurisdiction Type



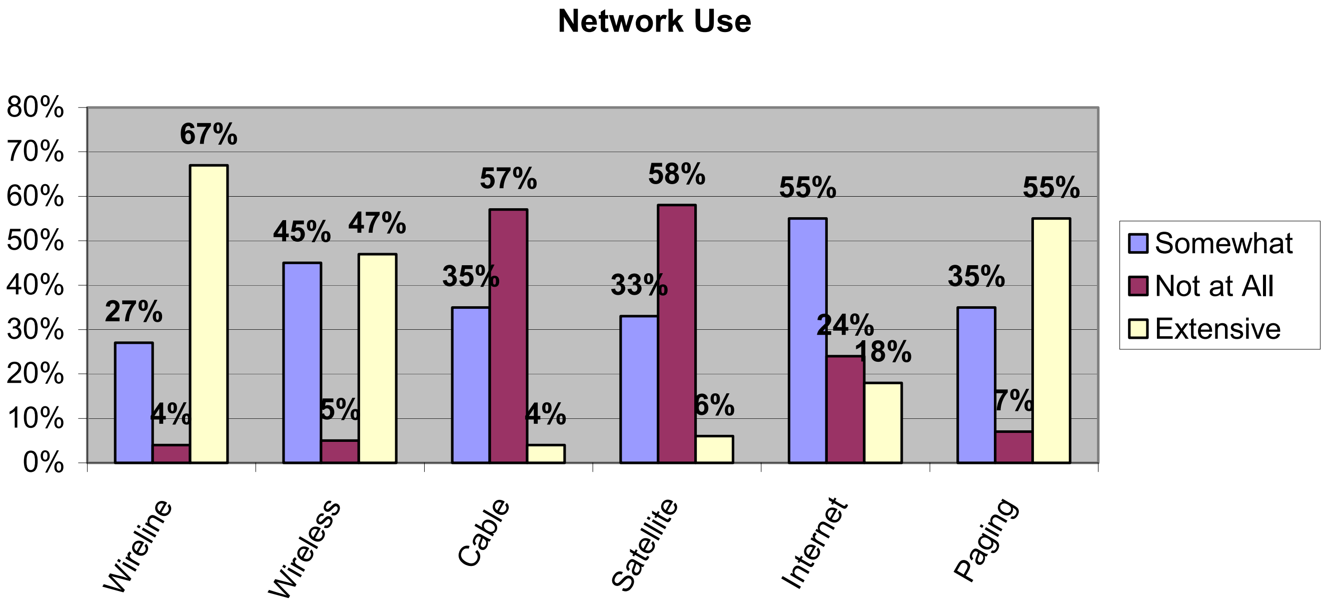
Years of Service



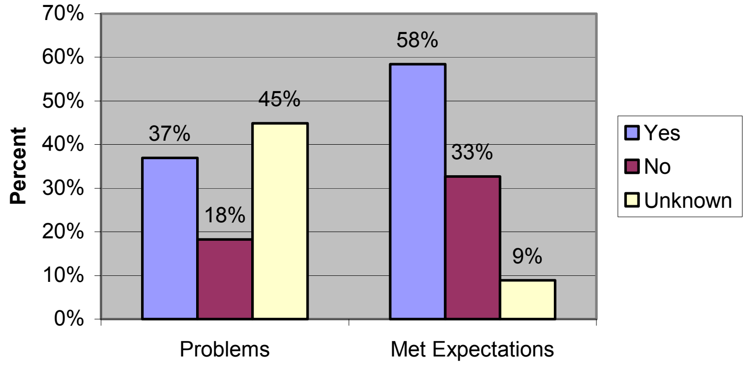


3.3.2 Experience with Commercial Networks

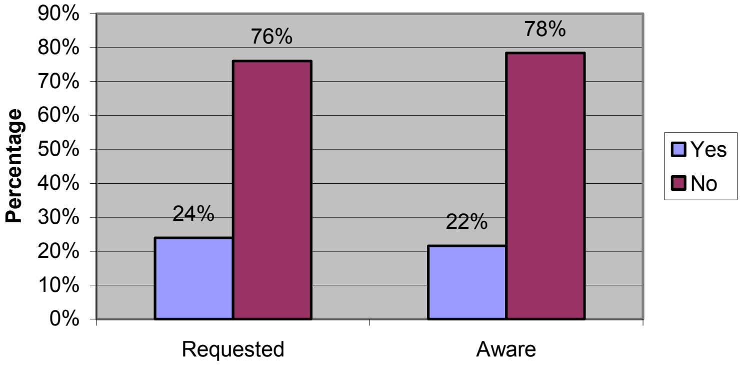
The survey included nine (9) multi-part questions concerning the Public Safety respondents experience with and use of commercial communications during critical incidents. The questions covered the basic what, when, why and how commercial communications are used during a crisis response. Topics covered in the questions included which networks were used and the extent to which they were used, the purpose of the communications, variation in usage as the incident progressed, with whom they were communicating, their experience with the commercial networks, and familiarity with and use of emergency services. The following charts represent Public Safety's responses.



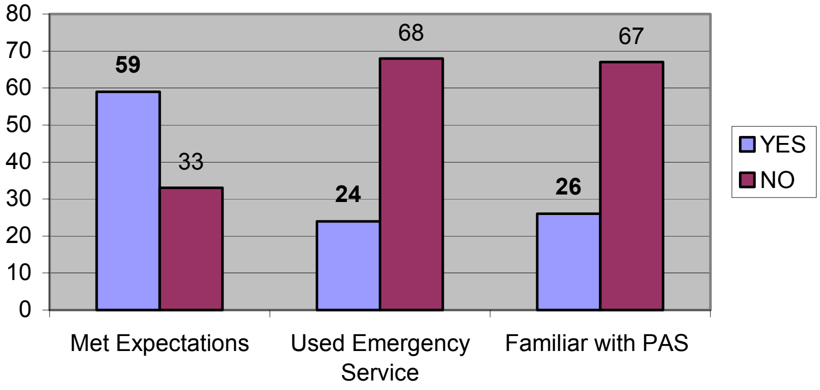
Commercial Network Performance



Emergency Telephone Services



Service Experience



3.4 Public Safety Interview Results

Upon completion of analysis of the survey data and comments, the Focus Group determined that there was a need to further clarify several points and validate the Group's interpretation of the data. Since the majority of the survey participants voluntarily included contact information as part of their survey response, the Group selected several participants with whom to conduct follow up interviews for this purpose. The interviews were conducted with:

- Chief Stephen McDonald – Nassau County (NY) Police Department
- Sgt. Paul Einreinhofer – Bergen County (NJ) Police Department
- Mr. David Troup – Director of Communications – Boston Police Department
- Mr. Steven Devine – Frequency Advisor/Radio Engineer – Missouri State Patrol
- Ms. Eva Luna, ENP – Communications Manager, City of Midland, Texas
- Mr. Charles O. Gibson – Director of Communications and Information Systems, City of Midland, Texas
- Mr. Bo Alexander – Public Safety Systems Administrator, City of Midland, Texas
- Mr. David Flores – Radio Technician, City of Midland, Texas

Appendix C2 contains a summary of the questions asked during the interview and the responses provided by these individuals.

4 Wireline Communications Subcommittee (also considers Cable and Internet)

4.1 Scope

The FG-1C Wireline Subcommittee was charged with assessing technology, documentation, tools and practices available to Public Switched Telephone Networks (PSTNs), generally referred to as wireline networks, which proactively and reactively impact the ability of the Public Safety sector to respond in times of extreme emergency or crisis and by extension the handling of day to day challenges. The Subcommittee explored actions necessary or desirable to ensure that commercial wireline communications service networks (in conjunction with wireless, satellite, and cable public telecommunications networks) can meet the needs of public safety emergency communications.

The findings of the FG-1C Cable Subcommittee are also included in this section. The findings of this subcommittee refer to Cable Television (CATV) service providers. As CATV networks have evolved over the previous decade, these networks now provide a multitude of services that include video, data, and telephony. Because CATV will continue to evolve and exploit technologies like VoIP and carry telephony services on a broader scale, it will be inevitably interwoven with the PSTN fabric, and thus it seemed appropriate that CATV be included as part of this section. When determining how CATV can meet the needs of public safety emergency communications, any networks offering telephony were considered "wireline networks" as well as CATV networks.

The FG-1C Wireline Subcommittee conducted an assessment of the commercial communications services needs of the Public Safety Community. First by identifying the role currently played by the wireline industry in supporting the private networks that are used by the Public Safety community, and secondly by incorporating the needs as articulated in survey responses by and interviews with Public Safety personnel. The data was gathered, sorted, analyzed and transferred to a matrix with categories addressing the various aspects of the PSTN including power, landline backbone, capacity utilization, coverage capability, redundancy, diversity, reliability, restoration, provisioning, awareness and utilization of existing services, and security. The matrix was also populated with the existing applicable BP's. Using this matrix, the Subcommittee performed a gap analysis allowing the FG-1C to identify shortfalls within the industry and identify opportunities where commercial wireline networks can assist the Public Safety community in more effective ways.

The expertise of the various participants of this Subcommittee, in conjunction with direct interaction with public safety personnel, allowed for the gathering of data on the current state of wireline networks, the first hand experience of the agencies that are impacted, and information on what enhancements the "users" would like to see deployed. The survey captured the commercial network requirements of public safety personnel, particularly first responders from agencies such as:

- Local, County, State and Federal Law Enforcement
- Local and County Fire Departments
- Emergency Medical Services
- Federal, State and Local Office of Emergency Management
- Communications Officers

The survey results formed the basis for the development of the Recommendations and Best Practices that are presented later in this document.

4.2 Industry Interaction and Best Practices

The FG-1C Wireline Subcommittee's efforts took on a three pronged approach:

- First, the assessment of how commercial wireline networks support the Public Safety community and identifying applicable existing NRIC V Best Practices. Once identified, these BPs were evaluated and if necessary modified to better meet the specific needs of the Public Safety community. In some instances, it became evident that new Best Practices would need to be developed.
- The second effort was to take results of the Public Safety Survey and identify the areas that commercial wireline applications could meet the needs as identified by the respondents of the survey and determine if BPs may already exist or could be developed.
- The third effort consisted of personal interviews with members of the Public Safety community. These interviews were comprised, of 6 questions, posed to 5 Public Safety officials. The responses generated by these interviews were also evaluated to identify the areas that commercial wireline applications would meet a need and again identify any existing BPs that might apply or could be developed.

The Best Practice search resulted in the identification of 39 Best Practices being applicable to wireline Public Safety; some of which require minor modifications to be apropos and one which requires modification but is outside the scope of Public Safety. (BP 5-522: ”Because of the environment of multiple Network Operators, multiple Service Providers and multiple Network Equipment suppliers, all of these parties are encouraged to participate in standards development. (e.g., IETF, NANOG)”) was referred to the Interoperability Focus Group. For the most part, our findings show that the Best Practices can be categorized as having a focus on:

- Training & Ongoing Test Drills
- PSAP, Equipment and Facility Diversity
- Communications
- Essential Service Prioritization or Restoration
- Survey and Wireline Results
- Survey and Cable Results

The need for seven additional wireline Best Practices was identified and will be included in the Key Findings section.

4.2.1 Training and Ongoing Test Drills

It must be recognized that the reach of previous NRIC recommendations and practices were generally limited to the communications industry. NRIC VI and in particular this Committee is incorporating private sector involvement in an unprecedented manner. The participants now include members of the public safety arena and emergency management agencies that until now have had limited if any interaction with NRIC. The challenge here will become the successful outreach to the various member agencies and the dissemination of information to an entirely new audience.

The need for education and training not only applies to Service Providers, Network Providers, Public Safety personnel but extends to general public as well. For example, as 311 is more widely deployed, the public should be made aware that 311 not only exists but should be educated as to its proper use. While 311 service is similar to 911, it is for non-emergency situations only. It is vital that the public understand, that using 311 vs. 911 allows 911 trained personnel to remain available for the true “life and death” or Homeland Security situations warranting their specialized skill set. This behavior will also minimize traffic congestion on the 911 dedicated networks and again, leave capacity available for true crisis situations.

Various BPs outline the need service providers, network providers, and equipment vendors to participate in a variety of training exercises and ongoing testing that ensures network reliability. Going forward, with regard to their reliance on commercial network elements and with their respective PSAPs, it would seem prudent to incorporate Public Safety personnel in these efforts. At minimum, on an annual basis, a cooperative effort should be initiated to test Contingency Plans. All personnel should be aware of the scope of the tests, yet the tests should be conducted “unannounced” in order to simulate the true impact of a disaster. Results should be documented, inclusive of “lessons learned” and weaknesses such that procedures can subsequently be improved.

4.2.2 PSAP, Equipment and Facility Diversity

The most robust set of existing Best Practices addressed the need for Facility and/or PSAP Diversity. No single point of failure should exist in the path linking network elements critical to the operations of a 911 network. This includes geographically diverse inter-office transport facilities provided by standby protection facility diverse from the primary facility or by utilizing digital cross-connect systems. A second alternative is the deployment of fiber ring topologies. While this aggregation of traffic opposes the diverse fiber transport concept, it also provides redundancy and a self healing network formed by a closed loop connected to the 2 adjacent nodes via duplex communication facility.

As was previously articulated, private networks utilized by Public Safety agencies quite commonly rely on facilities obtained from commercial service providers as part of their backbone infrastructure or as transport between various elements of the private networks. As an example, it is quite common for private radio networks to use commercial wireline facilities to link transmission towers or to link towers to their main transmission facility. Under this architecture, the survivability of the private network is tied to the reliability of the commercial service. As such, strategies for redundant facilities and diverse routing of facilities in these applications would be prudent. This would require the coordination of the commercial service and/or network provider, the private service and/or network provider and the public safety agency to first identify these architectures and subsequently apply strategies for redundancy and diversity, similar to those in place for 911 networks and PSAPs, where necessary. Existing BPs were modified to include this recommendation.

Above and beyond the redundancy and self-healing aspects of the 911 network would be the inclusion of the Traffic Operator Position System (TOPS) as a back up to the 911 tandem. If the 911 jurisdiction permits, an available alternate route to the Operator is quite reliable. Some will recognize the call as 911 and automatically route the call to the serving 911 tandem while others will have the operator respond to the call and warm transfer to the emergency services provider. Yet another configuration, and a lower cost solution, is to use the PSTN as a back up between the end office and the tandem. Applications are available to capitalize on adjunct devices to monitor primary trunk path integrity. If the primary path to the tandem is out of service, the call can be manually forwarded over the PSTN to a pre-defined directory number. The caller may be identified if the administrative line is equipped with caller id. While this alternative is achieving the goal of "call completion", it should be noted that it is not E911.

On the terminating end of a 911 call, diversity, back up and disaster recovery procedures are equally as important. There are several alternatives for insuring call completion to the PSAP. The most common is the programming of the tandem such that congestion immediately results in an automatic route to a pre-defined directory number of an alternative PSAP destination. This may terminate either in an administrative number or to the primary PSAP positions. A variation, on this arrangement, is the programming of the end office, thus engaging alternative route selection. Again, the end office could route to a pre-defined administrative number or a primary PSAP position.

A common solution to diversifying the path, to the PSAP, is dual tandem switching. This enables the calls, from the end offices, to be split between 2 tandems. This is further enhanced by diverse interoffice transport facilities. A more extreme and costly concept to enable "PSAP Diversity" or a Disaster Recovery plan is the investment in a mobile PSAP. To accommodate instances where the facilities are interrupted or it becomes necessary to evacuate the PSAP, some jurisdictions have invested in the mobile PSAP system connected to the phone jack at the serving end office. This connection is typically in a secure, but easily accessible location. Pre-arrangements with the LEC are paramount.

Equipment diversity should be implemented and preserved by the concept of "red tagging" to insure that all maintenance personnel are well aware of the importance and the need to retain or provision over several similar pieces of equipment. The "red tag" alerts the maintenance personnel that the equipment is used for critical, essential services and is to be treated with care.

4.2.3 Communications

The theme of "Communications" is also common within at least seven Best Practices. Suggestions as parochial as "service providers and network providers should maintain a "24 X 7" contact list of other service providers for service restoration purposes" to others which recommend strong linkage between the Service Providers and PSAPs, 911 administrators and public safety agencies. This team, be it on a state, county or community-wide basis, should routinely communicate, develop, review and update plans for 911 scenarios as well as participate in Industry or State held forums on improving reliability and security. This is the relationship necessary to form a unified emergency services network. Alliances should be continually strengthened to all network linkages considered vital to a community's ability to respond to emergencies. This includes communications from the PSAP to law enforcement dispatchers, to response personnel, to emergency medical service dispatchers, to response personnel, to fire fighter dispatchers, to hazardous material control centers, to trauma centers and emergency hospices. Consider the media as an ally in emergency times to solicit aid, establish standards to support interconnection from the PSAP to broadcast media organizations and local network repair centers. Media should be seen as a positive mechanism to alert the public during periods of emergencies through various public service announcement channels.

Also under the umbrella of communications, is Emergency Notification Systems (ENS). Calls from the Public Safety Sector, such as those from the PSAP to subscribers, are subject to being disabled because of calling features the subscriber may have purchased as enhancements to their basic telephone service. Best Practices were developed that attempt to deal with this situation.

Communications Best Practices can be taken to another level to ensure that the relationships established above and the communications infrastructure to implement a Disaster Recovery Plan are in place. Strategies, training, leadership roles & responsibilities, timely notifications to affected parties should facilitate orderly restoration in a network catastrophe.

4.2.4 Essential Service Prioritization or Restoration

All of the above "categories" of Best Practices are ultimately in support of service restoration in an orderly and prioritized manner. Service providers, equipment providers and personnel of the National Security and Emergency Preparedness (NSEP) community should work cooperatively to support Industry organizations to develop and implement National Security features and functionality. Service providers of critical services to NSEP should avail themselves to the

Telecommunications Electric Service Priority (TESP) restoration initiatives. This initiative helps insure state NSEP communications by enabling utility companies to identify critical national, state and local NSEP facilities which quality for priority restoration of electric service.

In summary, the subcommittee identified areas of need that were not addressed by existing Best Practices and are discussed in section 4.3.1, with proposed resolutions to these needs. The team also made enhancements to the following 10 NRIC V Best Practices to specifically embrace Public Safety and are discussed in section 4.3.2 and included in Appendix G.

• 6-6-509	• 6-6-586
• 6-6-511	• 6-6-599
• 6-6-512	• 6-6-619
• 6-6-513	• 6-6-655
• 6-6-580	• 6-6-747

The subcommittee also identified seven new Best Practices that address needs identified by Public Safety Providers. These new Best Practices are outlined in section 4.3.3, and are included in Appendix G1.

4.2.5 Survey and Wireline Results

The survey yielded much data that was specifically applicable to the wireline segment of the industry. Of interesting note was the fact that while 67% of survey participants expressed that wireline applications were relied upon extensively by their agencies, they were not considered reliable enough to be their primary network. In fact, in times of crisis, wireline networks were perceived as severely disrupted and grid locked. It was also the perception of survey participants that commercial networks principle focus is not Public Safety, but rather being a business entity, the focus is on financial viability. Financial concerns aside, survey participants offered suggestions for improvements to the existing networks and operations procedures for the industry in general, and as applicable to the wireline segment of the industry in particular.

When asked for suggestions for improvements to the status quo, the survey yielded a substantial number of comments. These comments ranged from “dynamically” transitioning control and access of the PSTN to Public Safety personnel to establishing a task force to manage communications interoperability. From a wireline perspective, the comments generally addressed issues regarding broadband capabilities including the use of Voice over Internet Protocols (VoIP). As an example, one suggestion proposed the establishment of separate Internet connections for public safety. The development of an Emergency Communications Network (ECN) that would provide a mechanism for utilities (communications, energy, etc) and governmental agencies, including Public Safety, to be simultaneously notified of an emergency or disastrous event and would provide a forum for collective work on issues was also proposed.

The most frequently articulated areas of concern specific to wireline networks, and by definition, Local Exchange Carriers (LECs) were:

- Lack of diverse an/or redundant routing to the PSAPs
- Test Bed and Strategy dependence on LEC cost recovery

- Survivability of diverse or alternate routing
- All too frequent cable cuts
- LEC to LEC interoperability problems
- Lengthy repair intervals
- Corporate bureaucracy seen as an impediment to field personnel getting the job done.

Of general concern was:

- While cooperation during a crisis is generally very good, day to day concerns are hampered by politics and/or corporate bureaucracy.
- First responders to a crisis are not assured of PSTN front line personnel cooperation.
- Interoperability of multiple vendors within a single system is perceived as an issue.
- Intermittent accidental or weather related failures are perceived as an issue.

With respect to familiarity with GETS, relatively few survey participants were aware of its availability (46%). Of those with access to GETS, use had been limited almost entirely to responding to the September 11th tragedy, with very successful results. And while September 11th did spark additional Public Safety agencies to apply for GETS, the long application process and the need for additional training were cited as possible impediments to a more ubiquitous rollout. In addition, GETS dependence on “dial tone” was viewed as a negative.

Outages caused by cable cuts were a hot button with many survey participants. However, the frequency with which they occur is seen as a given by many. Some survey participant did agree that stiffer penalties for cuts should be imposed, efforts at preventing problems have not met with much success. On county official responding to the survey stated that they have implemented microwave diversity in its effort to minimize failures caused by cable cuts.

The implementation of 311 for non-emergency calls to Public Safety surprisingly initiated more comments regarding funding of the initiative than on any operational concerns. There was agreement however on the need to educate the public, and on the potential benefits to 911 systems.

The deployment of Emergency Alert Systems met with mixed reviews. Negative perceptions seemed to be attributed mainly to inadequate training of personnel. In addition, notification failures were attributed to calling features, such as call blocking, that disable ”Community Emergency Notification”.

Again, this is a summary of the survey responses as they may impact the wireline segment of the communications industry. A more comprehensive look at the survey and its results can be found in Section 3 of this document.

4.2.6 Survey and Cable Results

The survey revealed that Cable currently does not play a large role in emergencies, 56% of the respondents indicated that they do not rely on Cable at all. While information gathered from the survey was sparse with regards to how Cable is used in emergency communications, the following were determined to be the primary modes:

- Broadcasting Emergency Alert System (EAS) messages
- Alternate source for local broadcast information
- Primary source for satellite weather and news
- Alternate connection for data where available
- Alternate connection for voice where available

EAS was seen as beneficial but under-utilized. This was thought to be attributable to lack of understanding of how and when to trigger EAS, which highlighted the need for more training and better communication between the Public Safety community and CATV providers.

Since CATV currently plays a relatively small role in emergency communications it was rarely blamed for any shortfalls by the survey respondents and seen more as an alternative to over-utilized networks in times of crisis offering a truly diverse connection in most cases.

4.3 Key Findings

The subcommittee identified areas of need that were not addressed by existing Best Practices and are discussed in section 4.3.1, with proposed resolutions to these needs also identified. These issues are also included in Appendix G2. The team also made enhancements to the following 10 NRIC V Best Practices to specifically embrace Public Safety and are discussed in Section 4.3.2 and included in Appendix G.

• 6-6-509	• 6-6-586
• 6-6-511	• 6-6-599
• 6-6-512	• 6-6-619
• 6-6-513	• 6-6-655
• 6-6-580	• 6-6-747

The subcommittee also identified 7 new Best Practices that address needs identified by Public Safety Providers. These new Best Practices are outlined in section 4.3.3, and are included in Appendix G1.

It should be noted that in many cases, the Best Practices and proposed resolutions to identified gaps in existing best practices included in this section should be considered to encompass both Wireline, wireless, and cable network types.

4.3.1 Proposed Recommendations for Issues Identified in Gap Analysis

Rationale for Recommendation NRIC VI-1C-01: The survey results and the follow up interviews identified a lack of awareness of the Government Emergency Telecommunications Service (GETS). Authorized personnel are given a calling card with an identification number. During times of congestion in the public telephone network, these callers are able to get a higher priority through the network, providing they can reach the 1+ (710) NCS-GETS number. GETS works for all technologies as long as the caller can get to the public network.

> **NRIC VI-1C-01:** The NCS (National Communications System) and NCC (National Coordination Center) should enhance GETS awareness training to the Public Safety community. State and local emergency management agencies should coordinate regular drills testing the procedures for use of GETS service by local agencies in order to train them on the use of the system and to rehearse communications links and protocols between agencies.

Rationale for Recommendation NRIC VI-1C-02: In a recent review of the public safety community's use of the Telecommunications Service Priority system, it was determined that only a very small percentage of 911 operators have enrolled in the program. Having TSP restoration priority placed on qualifying critical public safety circuits in advance of an outage is essential in times of disaster or when carriers have to allocate repair crews. For example, during the recovery efforts in NYC following the 9/11 attacks priority went to restoring circuits with TSP before non-TSP circuits. Carriers will not have prioritization systems that supercede TSP (Paraphrase of the Report & Order that created the TSP system.) In light of this, Service Providers should ensure that services are readily available.

> **NRIC VI-1C-02:** Awareness of TSP for Public Safety critical circuits should be enhanced. Service Providers should ensure that services are readily available.

Rationale for Recommendation NRIC VI-1C-03: The survey indicated that CATV networks provide an alternate source for voice and data. As CATV networks continue to evolve and these services become ubiquitous over the CATV network it is reasonable to assume that reliance upon these services will also increase. In preparation for this increased reliance, it is critical to have good communication with emergency operations personnel.

> **NRIC VI-1C-03:** CATV providers should identify, in coordination with emergency operations personnel, key facilities serving public safety needs and develop an emergency restoration plan prioritizing service restoration to these facilities.

Rationale for Recommendation NRIC VI-1C-04: The follow-up interviews indicated that the Emergency Alert System (EAS) was under-utilized in many cases because of a lack of understanding of how and when to trigger the system.

> **NRIC VI-1C-04:** CATV providers and local emergency operations personnel should meet periodically to discuss and agree upon methods, key words, and qualified personnel to trigger the Emergency Alert Systems (EAS).

Rationale for Recommendation NRIC VI-1C-05: The need for training was indicated not only to be when to use EAS but also the activation of EAS. This is to reinforce the significance of training CATV personnel.

> **NRIC VI-1C-05:** CATV providers should develop Emergency Alert Systems (EAS) training and conduct an annual qualification for all personnel operating EAS equipment.

Rationale for Recommendation NRIC VI-1C-06: Speed and reliability of communications networks can be critical in an emergency, especially in light of the network congestion that was experienced during the September 11, 2001 terrorist attacks. In light of this, service providers should work with government and Public Safety Service and Support providers and other utilities in the development of State Emergency Communications Networks in order to provide a process for key utilities and government emergency responders to communicate during disaster events. An example of this type of network is the Alerting and Coordination Network (ACN) that connects major service providers, equipment vendors and key government locations to aid in network restoration during times of crisis. More information can be found at: http://www.ncs.gov/acn/

> **NRIC VI-1C-06:** Service Providers should work with government and Public Safety Service and Support providers and other utilities in the development of uniform State Emergency Communications Networks, not inconsistent with and Federal Emergency Communications Networks, in order to provide a process for key utilities and government emergency responders to communicate during disaster events.

Rationale for Recommendation NRIC VI-1C-07: The survey results and follow up interview identified that many critical circuits were disrupted when excavations caused disruptions of critical Public Safety Service. The state and local governments have a wide variety of methods to address this issue. These range from heavy fines, minimal fines, and no legislation at all. There are two forums that address excavation outages - NRSC (Network Reliability Steering Committee) and the Common Ground Alliance. There needs to be a coordinated effort with State and local governments to implement into legislation the best practices recommendations of the NRSC and the Common Ground Alliance.

> **NRIC VI-1C-07:** Federal, State legislators and regulatory bodies should work to strengthen laws and enact stricter ordinances with stiffer fines regarding back-hoe fades and related cable cuts. These activities have a direct adverse impact on communication services and as a result, work needs to be done to reduce this daily common occurrence.

Rationale for Recommendation NRIC VI-1C-08: The survey indicated that cut cable was a major concern and perceived as a primary contributor to a lack of service during times of crisis. Placing cables in a common trench minimizes space used in the right-of-way (ROW) therefore minimizing exposure.

> **NRIC VI-1C-08:** CATV providers should participate/develop utility coordinating committees to facilitate construction practices such as joint trenching that will make efficient use of right of ways and increase awareness of underground facilities in order to reduce the occurrences of back hoe fade.

Rationale for Recommendation NRIC VI-1C-09:In times of emergency conditions the possibility exists that PSAP administrative lines could receive direct emergency calls from the public due to alternate routing, or calls directly dialed by the public as identified in NRIC Best Practice 5-569 or proposed Best Practice 6-6-3201. The ability of the PSAP to identify the caller's number and name using common calling name and number services could be restricted to due to a caller's option of not presenting their name and number for display for normal direct dialed calls. Since the PSAP is provided with full name and number information for Enhanced 911 calls, it may be appropriate to provide the caller ID level of calling information on calls to the PSAP's administrative lines that could be used for receiving emergency calls, regardless of the caller's privacy indicator for calling name and number display.

> **NRIC VI-1C-09:** Commercial Communications providers should consider developing service options that will deliver Calling Name and Number information to PSAP administrative lines regardless of the caller's originating privacy indicator. This option would allow PSAPs to identify potential emergency calls placed to their administrative lines during network re-routing, or other events that may cause the delivery of emergency calls to the PSAP's administrative lines. (Reference BP 5-569)

Rationale for Recommendation NRIC VI-1C-10: In times of extreme emergencies, Public Safety's communications capabilities, both private and public based, may be unavailable. The only alternative commercial communications service option may be to locate the nearest public coin phone location. In much the same way that local fire departments map out and keep track of fire hydrants, Public Safety providers could establish a list of public pay phones that could be accessed by Public Safety personnel for essential communications if all other forms of communications are unavailable during times of emergency.

> **NRIC VI-1C-10:** Pay Phone service providers should make available, and Public Safety and Service Providers should have access to, a list of all Public Pay/Coin Phone locations within the service providers applicable territories for use by any requesting Public Safety entity.

Rationale for Recommendation NRIC VI-1C-14: The Data Over Cable Service Interface Specification 2.0 (DOCSIS) allows for tiered levels of service by granting different levels of priority to users.

> **NRIC VI-1C-14:** Development of an equivalent to priority access services for public Internet access over CATV networks by PUBLIC SAFETY. (Reference BP 5-545).

Rationale for Recommendation NRIC VI-1C-15: Supports law enforcement officials in gathering information that may uncover illegal activities or terrorist plots. This proposal provides symmetry to the BP 6-5-505 which is concerned with collecting information via wiretaps.

> **NRIC VI-1C-15:** When required by law, CATV providers should have procedures in place to support collection of information from caching servers and back-office systems for court orders or other appropriate reasons. (Reference BP 6-5-505)

Rationale for Recommendation NRIC VI-1C-16: An overriding theme in many of the survey responses was regarding congested networks during a crisis. The proposal below recognizes the need for CATV networks to proactively monitor their data networks to identify various types of attacks aimed at causing congestion and unavailability.

> **NRIC VI-1C-16:** CATV providers should have procedures in place to identify and respond to harmful actions or traffic being routed through their network. (Reference BP 6-5-505)

Rationale for Recommendation NRIC VI-1C-18: Many surveys and follow up interviews reported a high incidence of critical circuits being disabled when service provider personnel used the facilities from these dial tone less circuits. The FG originally though that Best Practice 5-567 Red Tag protection was the solution for this issue. However, discussion among committee participants showed that red tagging was not the best solution due to the proliferation of red tagging that renders the practice inefficient. Appendix A has the original BP-5-567.

> **NRIC VI-1C-18:** The process of "red tagging" circuits by Service Providers needs to be revisited by each provider to insure critical / essential circuits have appropriate "red tag" identification. "Critical" should be defined in context of national emergency / public safety.

4.3.2 Recommended Revised Best Practices

Several existing Best Practices from NRIC V can be modified to specifically identify application and inclusion of Public Safety Services and Support Providers within the context of the Best Practice. Changes to the following Best Practices (*changes are identified in italics)* are proposed to embrace the requirements of the Public Safety community.

• 6-6-509	• 6-6-586
• 6-6-511	• 6-6-599
• 6-6-512	• 6-6-619
• 6-6-513	• 6-6-655
• 6-6-747	

6-6-509: Network Operators and Service Providers should develop and maintain operations plans that address network reliability issues. *Network Operators and Service Providers should proactively include Public Safety Service and Support providers when developing network reliability plans.*

6-6-511: Service Providers and Network Operators should provide training for their operations personnel on network-level troubleshooting. *Network Operators and Service Providers should proactively include Public Safety Service and Support providers when developing trouble reporting plans and subsequent training.*

6-6-512: Service Providers and Network Operators should perform periodic inspection of cable ways (e.g., through floor and through wall passage ways, sealing compounds, fire and water stopping, etc.). *Public Safety Service and Support providers should also perform these inspections at their communication centers.*

6-6-513: Service Providers and Network Operators should maintain a "24 hours by 7 days" contact list of other providers and operators for service restoration for interconnected networks. *Where appropriate, this information should be shared with Public Safety Service and Support providers.* The NIIF website is http://www.atis.org/atis/clc/niif.

6-6-586: Service Providers of critical services to National Security and Emergency Preparedness (NSEP) users should avail themselves of the Telecommunications Electric Service Priority (TESP) restoration initiative. The TESP initiative helps to ensure relatively stable NSEP communications by enabling utility companies to efficiently identify critical national, state and local NSEP telecommunications facilities that qualify for priority restoration of electric service. Therefore, by participating in the TESP initiative, telecommunications Service Providers, utility companies, state organizations, *and Public Safety Service and Support organizations* collectively serve to ensure that essential national defense and civilian requirements are met. More information on the TESP initiative can be obtained from the National Communications System (NCS) Office of Priority Telecommunications, Manager National Communications Systems, Attn: OPT/N3, 701 South Courthouse Road, Arlington, Virginia 22204-2198, on telephone 703-607-4932 or on the web at TESP@NCS.GOV.

6-6-599: Test a Network's Operational Readiness though planned drills or simulated exercises. Service Providers should conduct exercises periodically keeping the following goals in mind: The exercise should be as authentic as practical. Scripts should be prepared in advanced and team members should play their roles as realistically as possible. While the staff must be well prepared, the actual exercise should be conducted unannounced in order to test the responsiveness of the team members and effectiveness of the emergency processes. Also, callout rosters and emergency phone lists should be verified. Early in the exercise, make sure everyone understands that this is a disaster simulation, not the real thing! This will avoid unnecessary confusion and misunderstandings that could adversely affect service. It is particularly important to coordinate disaster exercises with other Service Providers, *Public Safety Providers* and vendors. It is very important immediately following the drill to critique the entire procedure and identify "lessons learned". These should be documented and shared with the entire team.

6-6-619: All Service and *Public Safety Providers* should develop and/or ensure that appropriate pre-plans with fire agencies exist for all equipment locations, communication centers, and provide automatic notification to local fire department.

6-6-655: Service Providers and electric utilities should plan jointly to coordinate hurricane and other disaster restoration work. *Service Providers should proactively include Public Safety Service and Support providers when developing disaster restoration and prioritization plans.*

6-6-747: Service Providers, Equipment Suppliers and *Public Safety Service and Support providers* should work together to establish reliability and performance objectives in the field environment.

Rationale for Changes to BP 5-580: Changes are proposed to specifically identify and include the critical circuits provided to Public Safety Service and Support Providers in providing point-to-point circuits that are utilized for their radio tower and relay facilities.

6-6-580: "Critical Response Link Redundancy/Diversity and Security - The redundancy and diversity concepts set forth in Best Practice 6-5-0566 should be applied to other network links considered vital to a community's ability to respond to emergencies. Security practices and concepts set forth in the Security Best Practices should be applied to the critical systems supporting Link Redundancy and Diversity. *Critical links include point-to-point private circuits used by Public Safety networks for radio site communications, but obtained from commercial landline communication providers.* Types of links that are critical to the provision of emergency aid include communication links from the PSAP location to:

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

Standards should be supported to address interconnection issues between PSAP and CMRS, cable television service providers.

<u>Media and Repair Link Redundancy/Diversity</u> - the redundancy and diversity concepts set forth in Best Practice 5-566 also should be applied to network links considered vital to a community's ability to respond to emergencies. Types of links that are critical to the provision of emergency aid during such events include communication links from the PSAP location to broadcast media organizations and local network provider repair centers.

Media organizations can alert the public during periods of emergency network degradation or outage through appropriately worded public service. In addition, dedicated network links and/or alternate accesses to network provider repair personnel will ensure that interruptions are known immediately and that repair personnel are mobilized expeditiously."

4.3.3 Proposed New Best Practices

Rationale for Proposed BP 6-6-3201: Many existing Best Practices (e.g. 5-566, 5-568. 5-569, 5-570) deal with issues for diverse and alternate routes on calls to 911 PSAPs. In the unlikely event that a 911 network function is unable to process calls to the PSAP, several local Commercial TV and radio broadcasters have developed plans to inform the public that emergency calls, that end users normally would place to 911, should be dialed directly to a PSTN network address (7/10 digits) that is provisioned at the PSAP.

6-6-3201: Commercial TV and radio broadcasters should work with Public Safety organizations (PSAPs) to have a disaster recovery action in place in the event of a commercial communications failure effecting their 911 network, to inform callers requiring emergency services that they should dial a 7/10 digit number to reach PSAP administrative lines.

Rationale for Proposed Best Practice 6-6-3202: Some Public Safety entities have the ability to launch mass calling events that could cause congestion issues in the public network. This proposed process will reduce the potential of switch overload and resultant call blocking that may impact emergency and other essential services.

> **6-6-3202:** The Service Provider and the Public Safety Agency or its agent, that utilize an Emergency Notification System (Public Safety Mass Calling) should have a pre-established procedure to notify all impacted network operators, prior to launching an alert event. This process will reduce the potential of switch overload and resultant call blocking that may impact emergency and other essential services.

Rationale for Proposed BP 6-6-3203: Many subscribers have call blocking/ screening features (e.g. Do Not Disturb) that prevent calls from being completed to their lines. PSAPs routinely attempt to call subscribers back who dial 911 and fail to stay on the line to provide essential information. In addition, during emergency situations, Public Safety may conduct Mass calling as part of Emergency Notification Systems. The call blocking / screening features prohibit the Public Safety from completing to these types of calls to subscribers with these features on their lines. Both Verizon and Qwest have implemented procedures that allow for the override of some wireline network based call blocking/screening features for calls made from PSAPs or Emergency Notification Systems.

> **6-6-3203:** To assist in the effectiveness of Emergency Notification Systems (Public Safety Mass Calling) and return calls from PSAPs, Service providers should consider developing options that allow for call delivery from Emergency Notification Services to subscribers with call blocking/screening services.

Rationale for Proposed BP 6-6-3204 : The "newer" N11 Services, such as 211, 311 and 511 should be appropriately socialized & publicized such that the public is made aware of what constitutes a true 911 emergency and when the situation warrants the alternatives of 211 (ex: Public Assistance, Information & Referral), 311 (ex: trash pick up, cat up a tree) and 511 (Traffic Conditions and Road Closures). The education process should emphasize that calling 911 for non-emergencies could limit the support to people who currently are experiencing life-threatening situations and desperately need the specialized skills of a 911 trained individual. Existing Best Practice 5-578 discusses the need for educating the public on 911 calls, with the recent deployment of other N11 services, it is even more important to provide a comprehensive education program that emphasizes all options available to the public for properly contacting emergency and public safety services.

> **6-6-3204 :** Service providers should work with Public Safety Service and Support providers to educate the public on the proper use of N11 Access codes (211, 311 and 511 services) such that it enables the 911 network and personnel to be exclusively focused on emergencies. Proper use of all N11 codes, including 911, prevents exhaustion of resources of emergency personnel on non-emergency situations. (Reference BP 5-578)

Rationale for Proposed BP 6-6-3205: Network congestion during times of crisis could impede first responders' ability to react to a disaster. Additionally, in light of network convergence, service providers, network providers and public safety organizations should participate in standards bodies such as Committee T1 that establish standards for Emergency Telecommunications Services (ETS). ETS is an initiative from the Federal Government so that public safety and first responders have a secure and easily accessible network during times of disasters or national emergencies. At the time of this report, the contribution submitted to Committee T1A1 by NCS does not include 911 service in ETS.

> **6-6-3205:** Service providers, network providers and public safety organizations should participate in standards bodies that establish standards for Emergency Telecommunications Services (ETS). ETS is an initiative from the Federal Government so that public safety and first responders have a secure and easily accessible network during times of disasters or national emergencies. 911 is considered a critical service during times of emergency and national disasters and should be included in standards being developed for ETS.

Rationale for Proposed BP 6-6-3209: Local broadcast news, weather, and EAS information provides critical information to a large population quickly in a crisis. By serving local broadcasters with a fiber connection, this information can still be distributed in the event of a failure in the broadcaster's transmission facilities.

> **6-6-3209:** Where practical, CATV facilities shall receive signals from off-air broadcasters via fiber as the primary source with automatic fail over to the off-air signal as the secondary source.

Rationale for Proposed BP 6-6-3210: The survey and follow-up interviews both indicated a value in having truly diverse connections for voice and data. CATV was noted as a viable alternative in areas where these services are available. CATV also serves as a primary source for video and EAS information. Since the Emergency Operation Centers often trigger the EAS it is critical for these Centers to monitor the distribution of this information.

> **6-6-3210:** Where practical, CATV service providers should serve Emergency Operations Centers with a CATV connection to provide video for viewing local weather and news information, a diverse connection to the Internet and a diverse telecommunications connection if such services are available on the network.

5 Wireless Communications Subcommittee (also considers Satellite and Paging)

5.1 Introduction

The FG-1C Wireless Subcommittee's examination of wireless services commenced with the premise of NRIC Best Practices—those practices that are vital to the reliability of the nation's public communications networks and services, with particular emphasis on the challenges faced by the Nation's public safety agencies. The work that evolved is a result of enormous research, thought and discussion by representatives of network operators, equipment providers, services providers and public safety agencies and organizations. These representatives shared the understanding of the Best Practice impact on systems, processes, organizations, networks, business operations, complex cost issues and the unique challenges of public safety agencies since the September 11, 2001 attack. The primary objective was to provide guidance from assembled industry/government expertise and experience, with the shared intention of doing what is best for effective use of the nation's commercial wireless networks by public safety.

Commercial wireless communications have a unique and broadening role in public safety communications. These services include cellular, satellite and paging (both one way and two-way systems), as well as a comprehension that calls seeking emergency assistance are increasingly placed over the wireless networks. What the Subcommittee's work demonstrated is that public safety agencies rely upon their own pervasive internal wireless infrastructure networks for a range of critical communications requirement and that the integrity and efficiency of these networks remains fundamental. What was shown was not a movement to commercial networks to meet such requirements, but an extensive and growing use of commercial networks that are important to the efficiency and effectiveness of how public safety meets its widening responsibilities since the September 11, 2001 attack. Wireless communications can have a dramatic effect in assisting a public safety agency. To this end, the Subcommittee's work in examining Best Practices reflects how wireless services can provide expanding services that result in a tangible contribution to public safety agencies carrying out their duties.

5.2 Key Findings

The analyses of the survey results and follow up interviews identified several issues for Public Safety. The Focus Group divided these issues into three areas:

- The first area is identified as a gap in wireless telecommunications current best practices. The Focus Group has identified recommendations for resolving issues in this area.
- The second area dealt with modifying existing best practices to fully embrace Public Safety.
- The final issue grouping had at least one service provider that had a process for addressing these issues. The resolutions for the final grouping are recommended best practices.

5.2.1 Recommended Revised Best Practices (changes made are in *italics*)

Rationale for modification of BP 5-575: With the advent of E911 Phase I & II additional databases are required to deliver information to the Public Safety Answering Point (PSAP) during call setup. The Global Mobile Location Center (GMLC) or the Mobile Positioning Center (MPC) will send the Longitude and Latitude defining the location of a mobile 911 caller to the Mobile Switching Center (MSC) and on to the PSAP. The GMLC/MPC databases should be treated with the same care and redundancies that the ALI databases use. See appendix L for a detailed description of Wireless E911.

> **Modified BP 6-6-575:** *Database Systems used in Public Safety like ALI (Automatic Line Identification) and MPC (Mobile Positioning Center*) should be deployed in a redundant, geographically diverse fashion (i.e., two identical ALI database systems with mirrored data located in geographically diverse locations). To improve ALI/*MPC* reliability, deployments of fully redundant Public Safety database systems, such that ALI/*MPC*

system hardware and/or software failure does not impair ALI*/MPC* data accessibility. When deployed with geographically diverse transport facilities, single points of failure may be eliminated. ALI*/MPC* data should be placed on fault tolerant and secure computer platforms to increase the reliability of ALI*/MPC* display retrievals. When possible, "hot spare" computers should be held in full reserve for catastrophic events.

Rationale For modification of BP 5-577: The MPC databases are as important as ALI databases and should be part of the contingency plan training. See appendix L for detailed description of Wireless E911

Modified BP 6-6-577: 911 Contingency Plan Training - Once a contingency plan is developed, it should be periodically tested. These tests can be of various types: desktop checks tests (using a checklist to verify familiarity of "what to do in case of"), procedures simulation test (similar to a fire drill, e.g., simulating a disaster and monitoring the response), actual operations test (cause an event to happen, e.g., power or computer failure and monitor the response), actual security checks to verify the security of the essential service nodes (e.g., access controls to the ALI *and MPC databases*). The importance of testing a contingency plan is critical to its success. An annual schedule of testing and evaluating written results is an excellent method of ensuring that a plan will work in the event of a disaster and for identifying weaknesses in the plan.

5.2.2 Recommended New Best Practices

Rationale for BP 6-6-3206: Priority Access Service (PAS): The survey results and follow-up interviews identified a lack of awareness of the Wireless Priority Access System (WPAS). WPAS would allow qualified first responders to have priority access in an emergency. Appendix I contains a detailed description of PAS.

FG-1C Wireless 6-6-3206 Communications service providers should continue to work with the federal government and public safety officials to speed the development and deployment of Wireless PAS (Priority Access Services) solutions for all commercial wireless technologies (e.g., cellular, personal communications service, third generation networks, paging, and other wireless data services) to maximize Wireless PAS coverage, increase ubiquity, and give NSEP users the flexibility to handle a variety of emergencies and disasters.

Rationale for Wireless Recommendations 3207 and 3208: The survey results and follow up interviews highlighted that many public safety entities could not use some commercial wireless services due to inadequate coverage in some incident locations. The following two recommendations are a result of this finding:

FG-1C Wireless Recommendation 3207: Commercial Wireless Service providers should consider the input of the local Public Safety community when Commercial Wireless Service providers set priorities for wireless coverage in areas of importance to the Public Safety community.

FG-1C Wireless Recommendation 3208: Commercial Wireless Service providers should consider the input of the local Public Safety community when Commercial

Wireless Service providers set the priorities of improvement of their wireless coverage so that Public Safety entities can augment their own communications with commercial wireless services for non-mission-critical communications. Examples of items to address include funding, zoning, and viability of deploying additional cell sites.

5.2.3 New Recommendations Not Currently In Place

Rationale for recommendation NRIC IV-1C-11: Since the September 11, 2001 attack, communications service providers have increased efforts to formulate wireless priority access structures for public safety officials in an emergency. The challenge presented is that the very environment where priority access is often sought is when there is heightened demand for wireless services overall. By working with federal, state and local officials to establish the proper balance, communications service providers have sought to raise the awareness of the initiative and the issues that accompany it. The survey results confirm the public safety's needs in this regard. Appendix J and Appendix K contain descriptions of two commercially available PAS offerings

> **New wireless recommendation NRIC IV-1C-11:** Service Providers that offer Wireless PAS (Priority Access Services) should work with the NCS and the public safety community to promote the awareness of communication options currently available to those that qualify for the service in the Public Safety Sector.

Rationale for Recommendation NRIC VI-1C-17: Satellite services can provide critical communications capability during an emergency, yet obtaining the needed satellite capacity quickly requires that arrangements with satellite carriers be worked out in advance. Additionally, as the operational procedure for deploying satellite resources in an emergency may differ from deploying terrestrial cellular and other facilities, procedures unique to satellites should be integrated into the response procedures. For example, since ground terminals are needed to provide emergency service over satellites, they need to be available when an emergency occurs. Aside from the preliminary work there is a need to determine a procedure for priority access of the available space segment, when needed for emergency or public safety services. Additionally, Network Operation Centers specifically designed to support Public Safety operations and shared among a large number of users in order to provide emergency services more effectively, should interface, if not be integrated into, with satellite network operations centers.

There are several satellite services that may be useful for Public Safety entities. These include:

- Direct Access User terminals
- Satellite monitoring devices that can detect chemical and biological, as well as radiation

A description of satellite services that may be of interest to public safety can be found in Appendix F.

> **Wireless Recommendation NRIC VI-1C-17:** To ensure satellite service availability during an emergency, preparation and planning are critical. To this end, satellite carriers should work with Federal, state and local public safety agencies (including NCC) to ascertain requirements and availability of space segment capacity and assist public

safety agencies in developing operational emergency procedures, including training personnel in how to expedite access to satellite facilities. Proper planning also encompasses provisioning and preparing ground terminals, both multiple user and individual user terminals, before an emergency, in order to gain satellite access quickly as well as integrating and/or interfacing satellite network operation centers with terrestrial facilities.

Rationale for NRIC VI – 1C –19: Preplanning and coordination are essential if the satellite services are to be used in an emergency.

Wireless Recommendation NRIC VI – 1C –19: To ensure satellite service availability during an emergency, preparation and planning are critical. The terrestrial network operation centers, the public safety operation centers, and the satellite operation centers, should hold pre-planning and coordination meetings to determine how they will coordinate if and when an emergency occurs.

6 Conclusion

The scope of the Focus Group's work encompasses core matters integral to the security and sustainability of public communications networks throughout the United States and the need for adequate public communications capacity to continue during events of stress, small and large, that may affect specific communities or the nation as a whole. Underlying this fundamental is the often overlooked reliance by federal, state and local public safety agencies on these public communications network to assists its response to an incident.

The importance of public safety's reliance on commercial carriers for specific services is often underestimated by both the providers and the government entities that utilize them. Commercial carriers do not just provide wireless and wireline services for routine voice and data communications: for the majority of public safety telecommunications systems, commercial carriers provide mission-critical backbone and interconnectivity services. The reliability and restorability of these services has become more critical in light of the events of September 11th. The Focus Group captured these critical requirements in the Best Practices recommended herein.

The Focus Group embraced a fundamental of the NRIC VI process- incorporate private and public sector interests in addition to the involvement of historical industry participants. Specifically, the Focus Group included the public safety sector and entities that provide service and equipment to the sector. The process the Focus Group pursued was fluid and evolved to a pragmatic perspective of examining areas that would bring tangible benefits to public safety agency use of commercial networks. Several areas examined do not fall squarely into one entity's responsibility, so that the Focus Group's work, including its recommendations, is as much about what industry can do as it is about what is available to public safety agencies and how cooperation of all interests is crucial.

The Focus Group's work in identifying opportunities where commercial networks can aid the Public Safety sector has a wide a range. There are recommendations directed to core redundancy and diversity needs of public safety as well as how information regarding established programs can be made available to public safety agencies. Several areas encourage industry and the public safety sector work more closely together to examine and resolve particular matters. The Focus Group believes its work reflects not only areas where public safety will benefit in the short term but also NRIC VI's commitment that this effort commence a continuing process by all interests.

7 Acknowledgements

The subject of this report is the result of recognition, on the part of the FCC, that commercial communications provide an important service to Public Safety in critical incident responses. As a part of NRIC VI, the FCC has taken the unprecedented step to create a Homeland Security Focus Group specifically dedicated to understand how Public Safety uses commercial communication services in times of crisis. The FCC charged the Focus Group to identify how these services can better meet Public Safety's needs.

This report and its key findings would not have been possible without the enthusiastic industry collaboration between the network operators, service providers, equipment vendors, industry associations and Public Safety organizations. The Focus Group participants, identified in Section 2.4 and in Appendix B, readily accepted the serious nature of this undertaking and its potential impact to save lives. Almost 3000 participant hours were expended in Focus Group and Subcommittee meetings to create the survey, analyze the data, determine Best Practices and write the report. In addition, many personal hours were spent by individuals outside of these meetings.

Special recognition is given here for the leaders of the Subcommittees who coordinated additional meetings, guided analysis of the data and supervised the review and creation of Best Practices and recommendations.

Wireline Subcommittee Leaders
Lance Thomason – SBC
Dale Morgenstern – AT&T
Doug Jones – Verizon

Wireless Subcommittee Leaders
Reeta Singh – AT&T Wireless
Tomas Bern – Ericsson

Cable and Internet Subcommittee Leader
Dan Sanders – Comcast

The Focus Group Chairs would like to recognize the following individuals for their support:

Pam Stegora-Axeberg – Steering Committee Chair, Qwest
Jeffrey Goldthorp – NRIC VI Designated Federal Officer, FCC

The Focus Group would also like to recognize the following organizations that provided assistance:

Association of Public-Safety Communication Officials-International
International Association of Police Chiefs
International Association of Fire Chiefs
National Public Safety Telecommunications Council
Public Safety National Coordination Committee
Public Safety Wireless Network

8 Appendices

Appendix A – Acronym List

ACN	Alerting and Coordination Network
ALI	Automatic Line Identification
APCO	Association of Public-Safety Communication Officials-International
ATIS	Alliance for Telecommunications Industry Solutions
BP; BPs	Best Practice(s)
CATV	Cable Television (Community Antenna Television)
CDPD	Cellular Digital Packet Data
CLEC	Competitive Local Exchange Carrier
CMRS	Commercial Mobile Radio Service
DCS	Digital Cross-connect Systems
E-911	Enhanced 911
EAS	Emergency Alert System
ECN	Emergency Communications Network
EMS	Emergency Medical Service
ENP	Emergency Number Professional
ENS	Emergency Notification Systems
ETS	Emergency Telecommunications Services
FCC	Federal Communications Commission
FG-1C	NRIC Focus Group 1C (Homeland Security: Public Safety)
GETS	Government Emergency Telephone Service
GMLC	Global Mobile Location Center
IACP	International Association of Chiefs of Police
IAFC	International Association of Fire Chiefs
IETF	Internet Engineering Task Force
ILEC	Incumbent Local Exchange Carrier
LEC	Local Exchange Carrier
MDUG	Motorola Data Users Group
MPC	Mobile Positioning Center
MSC	Mobile Switching Center
MTUG	Motorola Telecommunications Users Group

NANOG	North American Network Operators' Group
NCC	NCS/National Coordination Committee
NCS	National Communications System
NENA	National Emergency Number Association
NIIF	Network Connection Interoperability Forum
NMC	Network Management Center
NPSTC	National Public Safety Telecommunications Committee
NRIC	Network Reliability and Interoperability Council
NRSC	Network Reliability Steering Committee
NSEP	National Security and Emergency Preparedness
PAS	Priority Access Service
PBX	Private Branch Exchange
PCS	Personal Communications Systems
PSAP; PSAPs	Public Safety Answering Point(s)
PSNCC	Public Safety National Coordination Committee
PSTN	Public Telephone Switched Network
PSWAC	Public Safety Wireless Advisory Committee
PSWN	Public Safety Wireless Network
ROW	Right-of-Way
SLA	Service Level Agreement
SONET	Synchronous Optical Network
TESP	Telecommunications Electric Service Priority
TOPS	Traffic Operator Position System
TSP	Telecommunications Service Priority
VoIP	Voice over Internet Protocol
WPAS	Wireless Priority Access System

Appendix B – FG-1C Membership

Mike Roden (Co-Chair)	Cingular Wireless LLC
Don Dautel (Co-Chair)	Motorola
Tomas Bern	Ericsson
Rick Canaday	AT&T
Shawn Cochran	BellSouth
Ted Dempsey	APCO
Len Golding	Hughes Network Systems
Ed Hall	ATIS
James M. Hammill	Telcordia Technologies
Kenneth Helgeson	VeriSign
Roger Hixson	NENA
Douglas R. Jones	Verizon
James Lankford	SBC
John Logan	APCO
Ron Mathis	Intrado Inc.
Stephen Meer	Intrado Inc.
Dale Morgenstern	AT&T
Tom Munoz	Sprint
Glenn Nash	APCO
Dr. Barbara Reagor	Telcordia Technologies
Gee Rittenhouse	Lucent Technologies
Robert Ritter	Nextel Communications
Anthony M. Rutkowski	VeriSign
Dan Sanders	Comcast Cable Communications
Reeta Singh	AT&T Wireless
Doug Smith	Nextel Communications
James Turner	ATIS
Lance Thomason	SBC
Rachel Torrence	Qwest Communications
Georganne Weidenbach	Qwest Communications

Appendix C – Sample Survey and Interview Questions

Included below is the survey instrument used. Appendix C1 contains follow-up questions asked in interviews with selected respondents listed in Section 2.4 of the Report, and Appendix C2 contains a detailed account of their responses to those follow-up questions.

Public Safety Survey

Thank you for taking the time to share your experience. Your input will be an important contribution in the NRIC's recommendations to the FCC on securing communications to help you ensure America's safety. Individual responses will be kept confidential, and will be aggregated within a report to the NRIC Public Safety Focus Group.

Demographic Information

1. Please share your area of responsibility and position (check one per category):

Responsibility		Position	
Appointed/Elected Official		Administrative	
Combined Dispatch		Dispatch Operator	
EMS		Engineer/Technician	
Fire		Field Operations/Front Line	
Police		Manager	
Private Sector (Specify)		Supervisor	
City/County/State Operations		Communications Manager	
Other (Specify)		Other (Specify)	

2. Name of Agency:____

3. Number of Personnel in Agency:

   Less than 25 ______

   26-250 ______

   251-499 ______

   500+ ______

4. Jurisdiction:

   Local ____Regional ____Statewide ____ Nationwide ____

5. Is your jurisdiction primarily (check one):

   Urban____ Suburban____ Rural________

6. Years of Professional Experience:

Less than 5______ 6-15 ______ More than 15 ______

7. The subsequent questions concern the use of **commercial** networks during a **major response**. Please indicate from which perspective you will be answering the questions (check one):

   Incident Commander ______
   First Responder on Front Line ______
   Support Personnel ______
   Chief, Deputy Chief or Commanding Officer ______
   Other (specify)_____________________ ______

Commercial Networks Usage Information

The following questions focus on the **commercial** communication network (e.g. telephone, wireless, cable, satellite, Internet, paging) needs of public safety agencies during a **major response** such as one caused by natural disaster, terrorist attacks or similar events. Please consider both your **voice and data** needs.

1. During a **major response**, to what extent does your agency rely on the following **commercial** networks?

	Not at All	Somewhat	Extensive
Wireline (Telephone Network)			
Wireless (Cellular, PCS, Nextel, CDPD)			
Cable			
Satellite			
Internet			
Paging			

2. For those **commercial** networks that you rely on somewhat or extensively during a **major response**, with whom do you use them to communicate? **(Check all that apply)**

	Wireline (Telephone)	Wireless (Cellular, PCS, Nextel, CDPD)	Cable	Satellite	Internet	Paging
Communications Within Your Department						
Communications Within Your Agency						
Inter Agency Communications						
Media Contact						
Communication with Government Officials						
Emergency Notification to the Public						
Other (Please Specify)						

3. For those **commercial** communications networks that you rely on somewhat or extensively in a **major response**, which do you use at specific times during your response? **(Check all that apply)**

Hours	1st Hour	1-6	6-12	12-24	24-48	48-72
Wireline (Telephone Network)						
Wireless (Cellular/PCS/Nextel, CDPD)						
Cable						
Satellite						
Internet						
Paging						

4. Please characterize the types of communication you have when using **commercial** networks during a **major response**, and how they vary by time. For example, are they?

a. Urgent/tied to the immediate response and primarily with other first responder groups
b. Directive/linked to ongoing response & recovery with other groups besides first responders
c. Informative/updates to government support organizations and/or the media

Please feel free to use your own descriptions, or those outlined above.

First Hour	
1-6 Hours	
6-12 Hours	
12-24 Hours	
24-48 Hours	
48-72 Hours	

5. Have the **commercial** networks (as identified above) met your expectations? (yes/no)_____
   a. Have you encountered problems using the commercial networks? If yes, please describe:

   ____

   b. How can these be remedied?

   ____

6. What additional services would you find useful?

   ____

7. Has your agency used Emergency Telephone services? (yes/no)___
   a. If yes, are you familiar with GETS (Government Emergency Telephone Service) or TSP (Telecommunication Service Priority)? (yes/no) ____

b. If yes, what is your experience with these systems? ____________________
____

8. Are you familiar with wireless PAS (Priority Access Service)? (yes/no) _____
   a. If yes, what is its importance to your organization?
      None ___ Some ___ High ___

9. Have you experienced any problems with **commercial** network facilities (e.g.: telephone lines, fiber optic links, microwave links, etc.) that are used to connect equipment in your private radio system? If yes, please describe: ____________________________________
____
____

10. What else about your interaction with **commercial** networks would you like to share with the NRIC? ____
____
____

11. Can you recommend an incident commander from your agency that we can contact to conduct this survey?
    Name:____
    Phone:____
    E-Mail:____

Once again, thank you for your participation and support. If additional research is needed, may we contact you? Yes __ No ___
Name: ____
Agency:____
Address:____
Phone:____
E-Mail:____

Appendix C1: Public Safety Survey Follow Up Interview Questions:

Wireless Sub-Committee

- In what instances are satellite services typically used and how often? What are the most common reasons for not using these services?
- How often (%) are commercial wireless services utilized or required for primary? For back up? Is that sufficient to warrant ruthless preemption priority access queuing?
- Are one-way or two-way pagers preferred by Public Safety? Are they used more frequently as primary response options or secondary or only as back up?
- Would your agency be willing to pay for the additional costs related to the deployment of Wireless PAS (WPAS) for first responders and other emergency personnel?
- What other alternatives are currently used by your Public Safety agency?
- Survey results show Public Safety personnel that have access to GETS (Government Emergency Telephone Service) have had little occasion to use it. Would it be beneficial to run drills internal to Public Safety to practice use of GETS to not only test its effectiveness but also appreciate its potential value? What practical role, if any, could commercial wireless carriers play in making this a successful endeavor?
- Should training be provided on how to obtain and circumstances to use GETS for Public Safety operators? Who should be responsible for providing this training? Should it be made mandatory?
- Should training be provided on how to obtain and administer TSP (Telecommunication Service Priority) for Public Safety telecommunications? Who should be responsible for providing this training? Should it be made mandatory?
  - Should SLA (Service Level Agreements) be created for Public Safety locations that would define restoration procedures, areas of responsibility, define response time, and give a priority for repair or provisioning of Public Safety critical circuits where TSP does not apply?
  - Should critical circuits, especially those that do not have dial tone, be marked with protective covers in all locations such as cross-boxes, wiring closets, and wall outlets?

Wireline Sub-Committee

- If GETS service was made available to you:
would it be a tool you would use
would it solve any of your communication problems
- If TSP (restoration and provisioning) service was made available to you:
would it be a tool you would use
would it solve any of your communication problems
- Would the development of a state Emergency Communication Network (ECN) that would provide a mechanism for utilities (communications, energy, etc.) and government (i.e., Public Safety) to be

simultaneously notified of an emergency or disaster event and collectively work the issues on a conference bridge?

- Since back-hoe fades with resulting cable and fiber cuts has a direct adverse impact on the general public's ability to contact Public Safety in times of need and inhibiting Public Safety's ability to respond under these conditions, would you support having federal and state government (e.g., Regulatory Commissions, Attorney Generals office, etc.) eliminate loop holes and impose stiffer fines on those contractors that repeatedly cause these disruptions.

- Do you believe the use of a non-emergency access code, such as 311, would help reduce congestion on the public communications provided to the Public Safety personnel during crisis situations? Do you think the use of 311 non-emergency codes would cause more confusion during a crisis and not serve the needs of the public?

Appendix C2: Public Safety Survey Follow Up Interview Responses:

Questions	Official 1	Official 2	Official 3	Official 4	Official 5
In what instances are satellite services typically used and how often? **What are the most common reasons for not using these services?**	Use some, primarily for State nuclear disaster operations. Finds delay cumbersome. Also looked for remote area data communications	Has attempted sat phones, but did not work well due to differences in how the system works. Bankrupt companies. Would look into it for data circuits. Cost is very high. Does use C-Band to get FEMA feeds	Not using them, expense and others are not using them also not using GPS	Not using anything via satellite. Starting to look at these	Have a link to state law enforcement system using satellite and get warnings from national weather service and use satellite for timing – Radio, Telephone access
How often (%) are commercial wireless services utilized or required for primary? **For back up?** **Is that sufficient to warrant ruthless preemption priority access queuing?**	Not for primary, but sometimes for tactical liaison, task force. Also for non-traditional uses. Does think that in the right situation, preemption is valid	Primary is zero. Back-up for ancillary or complementary service. Has a pager group for alpha paging alerts	None for mission critical, yes for auxiliary or back up. At minimum queuing, has a reservation about preemption	Mostly for back-up. Mobile command center utilizes wireless for communications out. Some events do have the LEC provide fixed facilities brought in. Says current wireless carrier has offered "priority access" before and it worked well. Was able to get through on wireless as needed	Use for mobile substations for police department and police use cell phones extensively. Would want preemption and priority in an emergency
Are one-way or two-way pagers preferred by Public Safety? **Are they used more frequently as primary response options or secondary or only as back up?**	Have moved from 1-way to 2way, secondary basis, commercial, often several to cover the state. Two cities have local, rural is commercial	No tone only. Alpha numeric (see above), and 2-way pagers for managers	Secondary or back, enthusiastic about potential for 2-way paging, email and database access, not necessarily peer to peer, has concerns about latency	Using 1-way on their own system. Commercial systems were clogged in last emergency system. Not using 2-way systems. Uses commercial system where managers travel away from local coverage area	Pagers are used for notification and secondary function. Volunteer Fire department uses pages as primary

Questions	Official 1	Official 2	Official 3	Official 4	Official 5
Would your agency be willing to pay for the additional costs related to the deployment of Wireless PAS (WPS) for first responders and other emergency personnel?	Service would be useful, but not able to say about funding	Would expect Feds (and/or carriers) to fund development and deployment	Generally yes, but cautious. Not expecting as a free service	Would want to know the costs	Yes a benefit. Done on bases of community service for free
What other wireless alternatives are currently used by your Public Safety agency?	More involvement with EAS Amber alert. CDPD	Does not have any specific use. Working with group to get Nextel type device working at peer level	None	In house mobile data terminal system	Have a couple of channels for each cable networks and has cable override
Survey results show Public Safety personnel that have access to GETS have had little occasion to use it. Would it be beneficial to run drills internal to Public Safety to practice use of GETS to not only test its effectiveness but also appreciate its potential value? What practical role, if any, could commercial wireless carriers play in making this a successful endeavor?	Somewhat, but not a user personally. Does expect some users of the State and does expect it to be useful	Worked when they needed it. Has many folks in the agency with it. Yes to drills	Not familiar with GETS. Does expect to receive training. And should be included in drills	Not familiar. Unsure of value, perhaps has value for communications center	Did not know what GETS is. Have a need for a few to have the ability to use GETS
Should training be provided on how to obtain and circumstances to use GETS for Public Safety operators? Who should be responsible for providing this training? Should it be made mandatory?	Not expecting to do mass training, only to those that would need it	Yes, see above. Says it would not hurt, since LEC/Wireless carrier interfaces with agency	See above	Need awareness training	Public safety and city management team and emergency management team

Questions	Official 1	Official 2	Official 3	Official 4	Official 5
Should training be provided on how to obtain and administer TSP for Public Safety telecommunications? Who should be responsible for providing this training? Should it be made mandatory?	Not familiar with it, does not think any are any designated as TSP. Definitely would like to have this on some remote transmitter tie lines	LEC not certain on how to do this, but getting close. Does feel that LEC and PS needs training on TSP procedures. Training from all groups, NCS, LEC and PS	Would be willing to pay additional monies for TSP. Is not familiar with TSP specifics. Does need training and awareness on TSP capabilities	Not familiar with TSP and not aware of any circuits identified by NCS for TSP	Never heard of it. Need awareness training and definitely see a need. APCO & NENA
Should SLAs be created for Public Safety locations that would define restoration procedures, areas of responsibility, define response time, and give a priority for repair or provisioning of Public Safety critical circuits where TSP does not apply?	Thinks this would be of benefit in circuit restoration	No SLAs, has TSP (or will have) agreements. Did private circuits and radio tie lines	Is pursuing an SLA with LEC today	LEC has been responsive and not pursued an SLA	Use and have an escalation process in place. 95% of time SLA works too expensive
Should critical circuits, especially those that do not have dial tone, be marked with protective covers in all locations such as cross-boxes, wiring closets, and wall outlets?	Relationships with LECs to get these back on the air	Yes to red caps! And training on how to keep them in place. Has many instances, and occurs almost on a weekly basis. Tried microwave, yet funding has not been available. Has implemented back-up radio facilities and locations to mitigate the problem.	Absolutely. War stories are abundant	Had many of these issues with analog circuits. Since moving to T1 circuits, incidences have gone down significantly. Marking is double-edged in that invites curiosity	911 equipment room is locked and is not specially marked inside the building. Have three sites that are connected by microwave and not using leased circuits. Never lost a circuit
If GETS service was made available to you: would it be a tool you would use? would it solve any of your communication problems?	Believes it is in use and available, no outcries for more users	Yes, has used it and it did solve communications problems	Does want to add it to the “tool kit”. Does not have it now	Believes it is of value where dial tone exists, but cannot get through rest of the system	Not needed aside from a few special people

Questions	Official 1	Official 2	Official 3	Official 4	Official 5
If TSP service was made available to you: would it be a tool you would use? would it solve any of your communication problems?	Would like to have a more formal approach to the system in use today even though personal relationships have met most of the needs	Yes, Yes, not sure – TSP designated circuits, LEC does not have them identified in system yet	Definitely wants to pursue TSP for provisioning and it fills some gaps in SLA that he has now	Needs to take a look and should designate some circuits as TSP	Formalization of local practices is a good idea
Would the development of a state Emergency Communication Network (ECN) that would provide a mechanism for utilities (communications, energy, etc.) and government (i.e., Public Safety) to be simultaneously notified of an emergency or disaster event and collectively work the issues on a conference bridge?	Does already have a similar process. Has 8 adjacent states, so planning intra and inter State is a must. This plan is a formalization of what they do now	Brings a rep to the EOC to facilitate this issue. Has established similar communications but does not have LEC participation	Says this would be significant value to his agency	Sees where this would be beneficial. Encourages the use	State has a large number of counties. Therefore this becomes a local issue. Something like ECN is in place and instituted at the county level. It is a good Idea. Looking for a way to Communicate between different radio frequencies. (problem is between different private radio frequencies that different agencies use)

Questions	Official 1	Official 2	Official 3	Official 4	Official 5
Since backhoe fades with resulting cable and fiber cuts has a direct adverse impact on the general public's ability to contact Public Safety in times of need and inhibiting Public Safety's ability to respond under these conditions, would you support having federal and state government (e.g., Regulatory Commissions, Attorney Generals office, etc.) eliminate loop holes and impose stiffer fines on those contractors that repeatedly cause these disruptions.	Need more education on call before you dig. Definitely expect the contractor to pay fines	High emphasis on "Call before you dig". The system is not foolproof. Still have issues when items have been "identified".	Yes. Has gone to microwave to circumvent these types of issues. Took advantage of PCS relocation to upgrade their systems	Last event was where LEC dug up their own cable. Does not expect heavier fines will alter the outages. Has experience of good coordination reducing outages	Definitely, not that big of deal
Do you believe the use of a non-emergency access code, such as 311, would help reduce congestion on the public communications provided to the Public Safety personnel during crisis situations? Do you think the use of 311 non-emergency codes would cause more confusion during a crisis and not serve the needs of the public?	311 is active in one city. Knows there are 911 calls that are non-emergency. Also would like to see standardization of PS calls.	Great idea, but where does funding come from. Not strongly looking at	Does feel that communications needs off-load during crisis situations. Has specific experience in recent event. Does expect public to be able to sort this out	Funding would be an issue. Does see where pubic can shift not-emergency off of 911. His city does promote a 7 digit number for non-emergency	Try to do a lot of public communication and the same people that would answer 9-1-1 would have to answer 3-1-1. Use other means like cable TV to notify people.· It is a good idea to have a national 511 system for highway emergencies

Questions	Official 1	Official 2	Official 3	Official 4	Official 5
Use of EAS?	Has recently begun the Amber Alert system. Not specifically used EAS to provide information to the public. NWS recently added several transmitters across the state	Last time that EBS was invoked, system had been automated without communicating the new procedures (and it did not work). Person was dispatched but extensive delay in deployment. Not all commercial providers participating. Absolutely would like to get EAS pushed to wireless devices		not used it. State Police now has Amber Alert but not utilized it	

Appendix D – Meeting Summary

MEETING NUMBER	DATE	MEETING TYPE	GROUP
1	May 9, 2002	Conference Call	Main Group
2	May 21, 2002	Workshop (DC)	Main Group
3	June 5, 2002	Conference Call	Main Group
4	June 12, 2002	Workshop (DC)	Main Group
5	June 26, 2002	Conference Call	Main Group
6	July 15, 2002	Workshop (DC)	Main Group
7	July 31, 2002	Conference Call	Main Group
8	August 19-20, 2002	Workshop (DC)	Main Group
9	August 28, 2002	Conference Call	Main Group
10	September 4, 2002	Conference Call	Wireline Sub-committee
11	September 13, 2002	Conference Call	Wireline Sub-committee
12	September 16-17, 2002	Workshop (IL)	Main Group
13	September 23, 2002	Conference Call	Wireline Sub-committee
14	September 26, 2002	Conference Call	Wireless Sub-committee
15	September 30, 2002	Conference Call	Wireless Sub-committee
16	October 1, 2002	Conference Call	Main Group
17	October 3, 2002	Conference Call	Wireline Sub-committee
18	October 8, 2002	Conference Call	Main Group
19	October 16, 2002	Conference Call	Wireless Sub-committee
20	October 17, 2002	Conference Call	Wireline Sub-committee
21	October 21-22, 2002	Workshop (DC)	Main Group
22	October 28, 2002	Conference Call	Wireline Sub-committee
23	October 31, 2002	Conference Call	Main Group
24	November 7, 2002	Conference Call	Main Group
25	November 12, 2002	Conference Call	Wireless Sub-committee
26	November 15, 2002	Conference Call	Wireline Sub-committee
27	November 18-19, 2002	Workshop (DC)	Main Group
28	December 2, 2002	Conference Call	Main Group
29	December 16, 2002	Conference Call	Main Group
30	December 17 ,2002	Conference Call	Wireless Sub-committee
31	January 13, 2003	Conference Call	Main Group
32	January 20-21, 2003	Workshop (DC)	Main Group
33	January 24, 2003	Conference Call	Wireless Sub-committee
34	January 27, 2003	Conference Call	Wireline Sub-committee
35	January 31, 2003	Conference Call	Wireless Sub-committee
36	February 3, 2003	Conference Call	Main Group
37	February 5, 2003	Conference Call	Main Group
38	February 7, 2003	Conference Call	Wireless Sub-committee
39	February 14, 2003	Conference Call	Wireless Sub-committee
40	February 18, 2003	Conference Call	Main Group
41	March 3, 2003	Conference Call	Main Group
42	March 5, 2003	Conference Call	Main Group

Appendix E – Keyword Matrix

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

Because of the new emphasis on Homeland Security relating to public communications for Public Safety, new keywords were introduced in NRIC VI.

The Following for keywords were introduced by Focus Group 1C (FG1C) for use in identifying public communication issues for Public Safety.

Emergency Capacity Utilization
Diversity

Wireless Coverage Capability
Public Safety

Keyword	Definition of Keyword
Emergency Capacity Utilization	Issues relating to insuring adequate access to commercial services during periods of high usage. (wireless, local dial tone, LD trunking, GETS).
Wireless Coverage Capability	Issues relating to ensuring access and maintenance of adequate commercial service for access to public safety when and where requested or required (e.g. wireless coverage, spare facilities)
Diversity	Issues relating to providing communication services across multiple systems or services (secure alternate routes i.e. geographic, defining diversity of physical facilities including the conduits, ducts, manholes, transport, buildings, etc). Included are issues relating to private communication circuits from remote radio sites to the dispatch centers used for radio systems, E911, incoming call centers including local & long distance providers (i.e. fiber, coaxial lines, etc).
Public Safety	Issues that impact services provided to Public Safety Providers

This Appendix correlates the new and existing Best Practices that impact Public Safety to these new Keywords, which help individuals identify Best Practices associated with specific job functions.

	NRIC V Network Reliability Best Practices Keywords																Keywords introduced in NRIC VI								
	Policy	Industry Cooperation	Network Design	Network Interoperability	Network Provisioning	Network Operations	Technical Support	Network Elements	Essential Services	Security	Procedures	Transport Facilities	Power	Fire	Emergency Preparedness	Disaster Recovery	Emergency Capacity Utilization	Wireless Coverage Capability	Diversity	Public Safety	Redundancy	Disaster Recovery - Restoration	Documentation	Training	Facility Design
BEST PRACTICES INTRODUCED BY FG1C																									
6-6-3201	1	1							1		1				1		1			1	1			1	
6-6-3202	1	1							1		1				1		1	1		1			1	1	
6-6-3203	1	1	1	1					1		1									1			1	1	1
6-6-3204	1	1							1		1				1		1			1			1	1	
6-6-3205	1	1	1						1		1				1					1				1	
6-6-3206	1	1	1					1	1		1				1		1	1		1					1
6-6-3207		1	1						1						1				1	1	1				
6-6-3208		1	1						1						1				1	1	1				
6-6-3209			1								1								1	1	1				1
6-6-3210	1	1																		1					
MODIFIED AND EXISTING NRIC V BEST PRACTICES																									
6-5-505																				1					
6-6-509																				1	1		1		
6-6-511																				1				1	
6-6-512																				1					
6-6-513																				1		1		1	
6-5-522																				1			1		
6-5-545																	1			1					
6-5-646																			1	1	1				1
6-5-566																			1	1	1	1			1
6-5-567																				1			1	1	
6-5-568																			1	1	1				
6-5-569																			1	1	1				
6-5-570																	1		1	1	1				
6-5-571																			1	1					
6-5-572																	1		1	1	1				
6-5-573																			1	1					
6-5-574																				1		1		1	
6-6-575																	1		1	1					
6-5-576																				1			1	1	

	NRIC V Network Reliability Best Practices Keywords																Keywords introduced in NRIC VI								
	Policy	Industry Cooperation	Network Design	Network Interoperability	Network Provisioning	Network Operations	Technical Support	Network Elements	Essential Services	Security	Procedures	Transport Facilities	Power	Fire	Emergency Preparedness	Disaster Recovery	Emergency Capacity Utilization	Wireless Coverage Capability	Diversity	Public Safety	Redundancy	Disaster Recovery - Restoration	Documentation	Training	Facility Design
6-6-577																				1			1	1	
6-5-578																				1				1	
6-5-579																				1			1		
6-6-580																				1	1		1		
6-5-581																				1			1	1	
6-5-584																				1					
6-6-586																				1				1	
6-5-598																				1			1	1	
6-6-599																				1			1	1	
6-6-619																				1			1		
6-6-655																				1		1	1		
6-6-747																				1		1	1		
6-5-758																				1		1		1	

Appendix F – Survey Raw Data

The survey, as shown in Appendix C, was completed by a total of 227 respondents and their results were emailed to our focus group via a web server. The summary of results indicates the number of respondents before each question. You will notice that this result does not always equal 227. This is due to incomplete responses from some of the survey participants. For multiple choice responses the total number of responses indicated does not always equal the sum of the individual responses. If the respondent entered a blank or illegal response it was counted as a response in the total number but was not broken out as one of the possible choices.

A summary of demographic data and raw survey responses is located at the following URL: http://www.CLEC.org/fg/charter_vi/fg1/survey_results. There are two links located at this site:

1. The first link, "Demographic Data" tallies the responses from the "Demographic Information" section of the survey to give a cross-section of the range of experience and backgrounds of the respondents. This link also tallies the responses from a few of the key multiple-choice questions.
2. The second link, "Responses to Essay Questions" contains five files which strip the essay questions from individual surveys and compiles them together to simplify comparative analysis and readability.

A graphical summary of the survey responses can be found in the slide show at the following URL: http://www.CLEC.org/fg/charter_vi/fg1/CLEC_FG_1C_report_Dec06.ppt

Appendix G – Best Practices and Recommendations

These Appendices (G, G1, G2) list the Best Practices either identified or developed by CLEC VI for Public Safety.

In light of the current state of urgency, Service Providers, Network Operators, and Equipment Suppliers are encouraged to prioritize their review of these Best Practices and prioritize their timely, appropriate actions.

The CLEC Best Practices are intended to give guidance on how best to protect the U.S. communications infrastructure. Decisions of whether or not to implement a specific Best Practice are intended to be left with the responsible organization (e.g., Service Provider, Network Operator, or Equipment Supplier).

Mandated implementation of these Best Practices is *not* consistent with their intent. Appropriate application requires understanding of the Best Practice impact on systems, processes, organizations, networks, subscribers, business operations, complex cost issues and other considerations. With these important considerations regarding intended use, the industry is concerned that government authorities may inappropriately impose these as regulations or court orders. Because the CLEC Best Practices have been developed as a result of broad industry cooperation that engages vast expertise and considerable voluntary resources, such misuse of these Best Practices may jeopardize the industry's willingness to work together to provide such guidance in the future.

Modified Best Practices are highlighted and changes to the original are in *italics.*

Number	Best Practice
6-5-505	When required by law, Network Operators and Service Providers should have procedures in place to support wire taps for court orders, or for other appropriate reasons (e.g., property rights protection from harmful activity). Network Operators and Service Providers should have procedures in place to identify and respond to harmful actions or traffic being routed through their network.
6-6-509	Network Operators and Service Providers should develop and maintain operations plans that address network reliability issues. *Network Operators and Service Providers should proactively include Public Safety Service and Support providers when developing network reliability plans.*
6-6-511	Service Providers and Network Operators should provide training for their operations personnel on network-level trouble shooting. *Network Operators and Service Providers should proactively include Public Safety Service and Support providers when developing trouble reporting plans and subsequent training.*
6-6-512	Service Providers and Network Operators should perform periodic inspection of cable ways (e.g., through floor and through wall passage ways, sealing compounds, fire and water stopping, etc.). *Public Safety Service and Support providers should also perform these inspections at their communication centers.*

Number	Best Practice
6-6-513	Service Providers and Network Operators should maintain a "24 hours by 7 days" contact list of other providers and operators for service restoration for interconnected networks. *Where appropriate, this information should be shared with Public Safety Service and Support providers.* The NIIF website is http://www.atis.org/atis/clc/niif.
6-5-522	Because of the environment of multiple Network Operators, multiple Service Providers, and multiple network Equipment Suppliers, all of these parties are encouraged to participate in standards development (e.g., IETF, NANOG).
6-5-545	When available in standards and protocols, Service Providers and Network Operators should identify and prioritize national security and emergency services in packet networks.
6-5-646	No single point of failure should exist in paths linking network elements deemed critical to the operations of a network (with this design, two or more simultaneous failures or errors must occur at the same time to cause a service interruption).
6-5-566	Diverse Inter-office Transport Facilities – When all 911 circuits are carried over a common interoffice facility route, the Public Safety Answering Point (PSAP) had increased exposure to possible service interruptions related to a single point of failure (e.g., cable cut). The 911 circuits should be placed over multiple, diverse interoffice facilities. Diversification may be attained by placing half of the essential communication circuits on one facility route, and the other half over another geographically diverse facility route (i.e., separate facility routes). Option 1: Diverse Interoffice Transport Facilities with Standby Protection – A variation of the facility diversity architecture is deployment of a 1-by-1 facility transport system. This architecture is protected by a standby protection facility that is geographically diverse from the primary facility. Because no calls are lost while switching to the alternate transport facility during a primary route failure, this architecture is considered self-healing. Option 2: Diverse Interoffice Transport Facilities using Digital Cross-connect Systems (DCS) – Earlier NRC Focus Group recommendations suggested using Diverse Interoffice Transport Facilities from the called serving end office via two diverse DCS. This approach provides diversity and, due to the concentration by the DCS network elements, offers a less costly network solution. Option 3: Fiber Ring Topologies for 911 Circuits – Fiber optic network elements offer network service providers the ability to aggregate large amounts of call traffic onto one transport facility. Traffic aggregation opposes the diverse fiber transport recommendations defined in this document. However, fiber rings permit a collection of nodes to form a closed loop whereby each node is connected to two adjacent nodes via a duplex communications facility. Fiber rings can provide redundancy such that services may be automatically restored (self-healing), allowing failure or degradation in a segment of the network without affecting service. Bi-directional fiber rings are used in some metropolitan areas, ensuring essential communications service is unaffected by cuts to fibers riding on the ring. Ring features and functionality are part of the Synchronous Optical Network (SONET) technical requirements. When essential communications are placed on self-healing SONET rings, service interruptions are minimized due to the architecture employed. This is only true so long as single points of failure do not negate the architectural redundancies. Examples of single point of failures include bi-directional rings within the same route, transport, facility etc.

Number	Best Practice
6-5-567	Red-Tagged Diverse Equipment – Depending on LEC provisioning practices, the equipment in the central office can represent single points of failure. 911 circuits should be spread over similar pieces of equipment, and each plug-in-level components and frame termination should be marked with red tags. The red tags alert LEC maintenance personnel that the equipment is used for critical, essential services and is to be treated with a high level of care.
6-5-568	Option 1: Alternate PSAPs from the 911 Tandem Switch – A common method of handling PSAP-to-Tandem transport facility interruptions is to program the 911 tandem switch for alternate route selection. If the 911 caller is unable to complete the call to the PSAP, the tandem switch would automatically complete the call to a pre-programmed directory number of alternate PSAP destination. The alternate PSAP may be either administrative telephones or another jurisdiction's PSAP positions, depending on the primary PSAP's pre-arranged needs. Option 2: Alternate PSAPs from the Serving End Office – Another method of handling PSAP-to-Tandem transport facility interruptions is to program the end office for alternate route selection. If the 911 caller is unable to complete the call to the PSAP, the end office may automatically complete the call to a pre-programmed directory number of alternate PSAP destination. The alternate PSAP may be either administrative telephones or another jurisdiction's PSAP positions, depending upon the primary PSAP's pre-arranged needs.
6-5-569	Option 1: PSTN as a Backup for 911 Dedicated Trunks – To ensure that 911 is minimally affected by potential traffic congestion sometimes experienced in the PSTN, PSAPs commonly create dedicated private public safety networks. A low cost alternative for handling 911 calls during periods of failure in the end office-to-911 tandem transport facility, is to use the PSTN as a backup between the caller's end office and the 911 tandem switch. Such applications may or may not make use of adjunct devices that monitor primary trunk path integrity. If the primary path to the 911 tandem switch should be interrupted or all-trunks-busy, the call may be forwarded over the PSTN to a preprogrammed directory number. Further, the caller may be identified if the administrative line is equipped with a caller identification (ID) device. Option 2: Wireless Network as Backup for 911 Dedicated Trunks – Similar to PSTN backup for completing 911 calls when the primary transport facility is interrupted, wireless networks may provide more diversity than the PSTN alternative.
6-5-570	Intraoffice 911 Termination to Mobile PSAP – Commonly, the transport facility between the PSAP and the serving end office may not have facility route diversity. To accommodate instances where these facilities are interrupted or it becomes necessary to evacuate the PSAP location, some PSAPs have established mobile PSAP systems that may be connected to phone jacks a the serving end office. The phone jacks, although usually installed inside the end office for security purposes, are typically installed in an accessible location for ease in locating them during an emergency. Some PSAPs have pre-arranged with the serving LEC to permit a jurisdictional employee having an emergency vehicle (e.g., police car) equipped with radio capability to retain a key to the LEC's end office and to connect to an RJ-11 jack for 911 call interception. Another type of receptacle may be pre-installed in the end office for connection to a mobile PSAP.

Number	Best Practice
6-5-571	Dual Active 911 Tandem Switches – Dual Active 911 tandem switch architectures enable circuits from the callers serving end office to be split between two tandem switches. Diverse interoffice transport facilities further enhance the reliability of the dual tandem arrangement. Diversity is also deployed on the interoffice transport facilities connecting each 911 tandem to the PSAP serving the end office.
6-5-572	Traffic Operator Position Systems (TOPS) as a 911 Tandem Backup – Operator services tandem switches can also serve as backup and/or overflow for network elements, due to their ubiquitous connectivity throughout the telephone network. In most instances, existing trunking and translations may be used when adding a TOPS to the 911 network. When an interoffice transport facility fails or an all-trunks-busy condition occurs, the backup/overflow route to the operator services tandem is selected. The operator tandem switch recognizes the call as an emergency by translating the 911 dialed digits, and may be pre-programmed to automatically route the call to the serving 911 tandem switch. Further, if the operator tandem switch is unable to access the 911 tandem switch, the call will automatically be “looped around” so that an operator may manually answer the call and manually attempt to reach an emergency services provider.
6-5-573	Local Loop Diversity – The local loop access is defined as that portion of the network which connects the caller (I.e., the subscriber to the PSAP) to the network serving end office. The local loop is potentially a single point of failure. Although it is unlikely the subscriber will purchase diverse transport facilities for typical PSTN service, PSAP local loops should be diverse where possible and/or make use of wireless technologies as a backup for local loop facility failure (e.g., cable cuts).
6-5-574	Network Management Center and Repair Priority – Network management centers (NMCs) should remotely monitor and manage the 911 network components. The NMCs should use network controls where technically feasible to quickly restore 911 service and provide priority repair during network failure events.
6-6-575	Diverse Automatic Location Identification *used in Public Safety, like* ALI (Automatic Line Identification) *and MPC (Mobile Positioning Center)* should be deployed in a redundant, geographically diverse fashion (i.e., two identical ALI*/MPC* database systems with mirrored data located in geographically diverse locations). *To improve ALI/MPC reliability, deployments of fully redundant Public Safety database systems, such that ALI/MPC* system hardware and/or software failure does not impair ALI*/MPC* data accessibility, will further improve ALI*/MPC* reliability. When deployed with geographically diverse transport facilities, single points of failure may be eliminated. ALI*/MPC* data should be placed on fault tolerant and secure computer platforms to increase the reliability of ALI*/MPC* display retrievals. When possible, “hot spare” computers should be held in full reserve for catastrophic events.

Number	Best Practice
6-5-576	Move Mass Calling Stimulator away from 911 Tandem Switch – Mass calling events may cause 911 service interruptions. Service interruptions caused by media stimulated calling has prompted the LECs to reassess and improve the handling of mass calling events. The 911 tandem switch series as the most critical network element in providing 911 service. If a media stimulated mass calling event is served by a 911 tandem, the PSAPs being served by the 911 tandem may experience delayed dial tone when call transfer is attempted by the PSAP personnel. The PSAP may also experience delays in call completion (ring-back tone) or a fast busy signal, which indicates that the call has failed to complete. To mitigate such instances, high volume call events should be moved to another end office. Pre-Planning for Mass Calling Events – To minimize the potential of interruption caused by media driven mass calling events, the LEC can identify periods of low call volume traffic so that the media may schedule mass calling events during low traffic periods. Carrier external affairs and marketing groups should work closely with media organizations to ensure 911 callers are unaffected by mass calling events.
6-6-577	"911 Contingency Plan Training – Once a contingency plan is developed, it should be periodically tested. These tests can be of various types: • desktop check tests (using a checklist to verify familiarity of "what to do in case of"), • procedures verification test (verify that established procedures are followed in a simulation), • simulation test (similar to a fire drill, e.g., simulating a disaster and monitoring the response), • actual operations test (cause an event to happen, e.g., power or computer failure and monitor the response), • actual security checks to verify the security of the essential service nodes (e.g., access controls to the ALI *and MPC databases*). The importance of testing a contingency plan is critical to its success. An annual schedule of testing and evaluating written results is an excellent method of ensuring that a plan will work in the event of a disaster and for identifying weaknesses in the plan. Close cooperation between a Service Provider and the PSAP in conducting actual operations testing will be of mutual benefit to both the Service Provider and the PSAP. An annual comprehensive operational test of the contingency plan is strongly encouraged."

Number	Best Practice
6-5-578	Educate the public on proper use of essential communications – The public's proper use of 911 service is critical to the effectiveness of the emergency network's operation. Misuse of 911 could lead to the following: congestion of the 911 network, leaving callers with real emergencies unable to contact a 911 operator, exhaustion of resources on non-emergency situations, reduction in a jurisdiction's ability to respond to emergency situations in a timely manner because of the jurisdiction's emergency response agencies being overwhelmed by responses to non-emergency situations. This could have potentially disastrous effects on the public's perception of its emergency network and emergency response agencies.
6-5-579	Improve communications among all Service Providers and PSAPs – Service Providers, 911 administrators, and public safety agencies should continually strive to improve communication among themselves. The team should routinely develop, review, and update disaster recovery plans for 911 disruption contingencies, share information about network and system security and reliability, and determine user preferences for call overflow routing conditions. They should actively participate in industry forums and associations focused on improving the reliability and security of emergency services and the development of technical industry standards. The National Emergency Number Association (NENA) and the Association of Public Safety Communications Officials (APCO) are two of the organizations that are open to all stakeholders of 911 service delivery and are focused on finding 911 solutions for emerging technologies (e.g., wireless, PBX, CLEC).

Number	Best Practice
6-6-580	“Critical Response Link Redundancy/Diversity and Security – The redundancy and diversity concepts set forth in Best Practice 6-5-0566 should be applied to other network links considered vital to a community’s ability to respond to emergencies. Security practices and concepts set forth in the Security Best Practices should be applied to the critical systems supporting Link Redundancy and Diversity. *Critical links include point-to-point private circuits used by Public Safety networks for radio site communications, but obtained from commercial landline communication providers*. Types of links that are critical to the provision of emergency aid include communication links from the PSAP location to: • Law enforcement dispatchers and/or response personnel. • Emergency medical service (EMS) dispatchers and ambulance response units. • Fire fighter dispatchers and response personnel. • Hazardous material control centers and other agencies offering remote diagnostic information and advice on how to respond to requests for emergency aid. • Trauma centers and similar emergency hospices. Standards should be supported to address interconnection issues between PSAP and CMRS, cable television service providers. Media and Repair Link Redundancy/Diversity – the redundancy and diversity concepts set forth in Best Practice 5-566 also should be applied to network links considered vital to a community’s ability to respond to emergencies. Types of links that are critical to the provision of emergency aid during such events include communication links from the PSAP location to broadcast media organizations and local network provider repair centers. Media organizations can alert the public during periods of emergency network degradation or outage through appropriately worded public service. In addition, dedicated network links and/or alternate accesses to network provider repair personnel will ensure that interruptions are known immediately and that repair personnel are mobilized expeditiously.”
6-5-581	Private Switch (PS)/Alternative LEC (CLEC) ALI – ALI data for alternate providers (e.g., PS, CLEC) should be included in the ALI systems. PSAPs have become increasingly reliant on the ALI data administered by the LECs, and believe that those individuals served by private telecommunications providers and/or alternate LEC providers should have their address information contained in their ALI database systems. The NENA Recommended Protocols for Data Exchange were established to enable ALI data integration of these providers.
6-5-584	Service Providers, Equipment Suppliers and representatives of the National Security and Emergency Preparedness (NSEP) community should work together to support appropriate industry and international organizations to develop and implement NSEP features and functionality in packet networks.

Number	Best Practice
6-6-586	Service Providers of critical services to National Security and Emergency Preparedness (NSEP) users should avail themselves of the Telecommunications Electric Service Priority (TESP) restoration initiative. The TESP initiative helps to ensure relatively stable NSEP communications by enabling utility companies to efficiently identify critical national, state and local NSEP telecommunications facilities that qualify for priority restoration of electric service. Therefore, by participating in the TESP initiative, telecommunications Service Providers, utility companies, state organizations, *and Public Safety Service and Support organizations* collectively serve to ensure that essential national defense and civilian requirements are met. More information on the TESP initiative can be obtained from the National Communications System (NCS) Office of Priority Telecommunications, Manager National Communications Systems, Attn: OPT/N3, 701 South Courthouse Road, Arlington, Virginia 22204-2198, on telephone 703-607-4932 or on the web at TESP@NCS.GOV.
6-5-598	Develop crisis management exercises – Service Providers should, at minimum have a communications structure in place for timely notification of affected parties in the event of disasters or emergencies. During the past several years a number of disastrous events have prompted an increased awareness on the part of all members of the telecommunications industry to the critical need to have a Disaster Preparedness strategy. This strategy should outline a network Service Provider's Disaster Preparedness organization, the roles, responsibilities and training of its members and provide for cooperative interaction among both internal and external organizations. The purpose of this strategy is to provide for the development of emergency plans that protect employees, ensure service continuity and provide for the orderly restoration of critical services in the event of a major network catastrophe.
6-6-599	Test a Network's Operational Readiness though planned drills or simulated exercises. Service Providers should conduct exercises periodically keeping the following goals in mind: The exercise should be as authentic as practical. Scripts should be prepared in advanced and team members should play their roles as realistically as possible. While the staff must be well prepared, the actual exercise should be conducted unannounced in order to test the responsiveness of the team members and effectiveness of the emergency processes. Also, callout rosters and emergency phone lists should be verified. Early in the exercise, make sure everyone understands that this is a disaster simulation, not the real thing! This will avoid unnecessary confusion and misunderstandings that could adversely affect service. It is particularly important to coordinate disaster exercises with other Service Providers, *Public Safety Providers* and vendors. It is very important immediately following the drill to critique the entire procedure and identify "lessons learned". These should be documented and shared with the entire team.
6-6-619	All Service and *Public Safety Providers* should develop and/or ensure that appropriate pre-plans with fire agencies exist for all equipment locations, communication centers, and provide automatic notification to local fire department.
6-6-655	Service Providers and electric utilities should plan jointly to coordinate hurricane and other disaster restoration work. *Service Providers should proactively include Public Safety Service and Support providers when developing disaster restoration and prioritization plans.*
6-6-747	Service Providers, Equipment Suppliers and *Public Safety Service and Support providers* should work together to establish reliability and performance objectives in the field environment.

Number	Best Practice
6-5-758	If 911 Call Completion is affected, test calls should be made by the Service Provider to the PSAP(s) to assess the impact. Once service is restored, the Services Provider should make multiple 911 test calls to ensure they complete properly.

Appendix G1 – Proposed New Best Practices

Number	Proposed New Best Practice
6-6-3201	Commercial TV and radio broadcasters should work with Public Safety organizations (PSAPs) to have a disaster recovery action in place in the event of a commercial communications failure affecting their 911 networks, to inform callers requiring emergency services that they should dial a 7/10 digit number to reach PSAP administrative lines. (Reference – Best Practices 5-577, 5-579, 5-598, 5-599)
6-6-3202	The Service Provider and the Public Safety Agency or its agent, that utilize an Emergency Notification System (Public Safety Mass Calling) should have a pre-established procedure to notify all impacted network operators, prior to launching an alert event. This process will reduce the potential of switch overload and resultant call blocking that may impact emergency and other essential services.
6-6-3203	To assist in the effectiveness of Emergency Notification Systems (Public Safety Mass Calling) and return calls from PSAPs, Service providers should consider developing options that allow for call delivery from Emergency Notification Services to all subscribers, including subscribers with call blocking/screening services.
6-6-3204	Service providers should work with Public Safety Service and Support providers to educate the public on the proper use of N11 Access codes (211, 311 and 511 services) such that it enables the 911 network and personnel to be exclusively focused on emergencies. Proper use of all N11 codes, including 911, prevents exhaustion of resources of emergency personnel on non-emergency situations. (Reference BP 5-578)
6-6-3205	Service providers, network providers and public safety organizations should participate in standards bodies that establish standards for Emergency Telecommunications Services (ETS). ETS is an initiative from the Federal Government so that public safety and first responders have a secure and easily accessible network during times of disasters or national emergencies. 911 is considered a critical service during times of emergency and national disasters and should be included in standards being developed for ETS.
6-6-3206	Communications service providers should continue to work with the federal government and public safety officials to speed the development and deployment of Wireless PAS (Priority Access Services) solutions for all commercial wireless technologies (e.g., cellular, personal communications service, third generation networks, paging, and other wireless data services) to maximize Wireless PAS coverage, increase ubiquity, and give NSEP users the flexibility to handle a variety of emergencies and disasters.
6-6-3207	Commercial Wireless Service providers should consider the input of the local Public Safety community when Commercial Wireless Service providers set priorities for wireless coverage in areas of importance to the Public Safety community.
6-6-3208	Commercial Wireless Service providers should consider the input of the local Public Safety community when Commercial Wireless Service providers set the priorities of improvement of their wireless coverage so that Public Safety entities can augment their own communications with commercial wireless services for non-mission-critical communications. Examples of items to address include funding, zoning, and viability of deploying additional cell sites.
6-6-3209	Where practical, CATV facilities shall receive signals from off-air broadcasters via fiber as the primary source with automatic fail over to the off-air signal as the secondary source.

Number	Proposed New Best Practice
6-6-3210	Where practical, CATV service providers should serve Emergency Operations Centers with a CATV connection to provide video for viewing local weather and news information, a diverse connection to the Internet and a diverse telecommunications connection if such services are available on the network.

Appendix G2 - Proposed Recommendations to Issues Identified in Gap Analysis

Number	Proposed Recommendations to Issues Identified in Gap Analysis
NRIC VI-1C-01	The NCS (National Communications System) and NCC (National Coordination Center) should enhance GETS awareness training to the Public Safety community. State and local emergency management agencies should coordinate regular drills testing the procedures for use of GETS service by local agencies in order to train them on the use of the system and to rehearse communications links and protocols between agencies.
NRIC VI-1C-02	Awareness of TSP for Public Safety critical circuits should to be enhanced. Service Providers should ensure that services are readily available.
NRIC VI-1C-03	Operators should identify, in coordination with emergency operations personnel, key facilities serving public safety needs and develop an emergency restoration plan prioritizing service restoration to these facilities. (Recommendation – reference existing BPs)
NRIC VI-1C-04	CATV providers and local emergency operations personnel should meet periodically to discuss and agree upon methods, key words, and qualified personnel to trigger the Emergency Alert Systems (EAS).
NRIC VI-1C-05	CATV providers should develop Emergency Alert Systems (EAS) training and conduct an annual qualification for all personnel operating EAS equipment.
NRIC VI-1C-06	Service Providers should work with government and Public Safety Service and Support providers and other utilities in the development of uniform State Emergency Communications Networks, not inconsistent with and Federal Emergency Communications Networks, in order to provide a process for key utilities and government emergency responders to communicate during disaster events.
NRIC VI-1C-07	Federal and State legislators and regulatory bodies should work to strengthen laws and enact stricter ordinances with stiffer fines regarding back-hoe fades and related cable cuts. These activities have a direct adverse impact on communication services and as a result, work needs to be done to reduce this daily common occurrence. (BP 5-567)
NRIC VI-1C-08	CATV providers should participate/develop utility coordinating committees to facilitate construction practices such as joint trenching that will that will make efficient use of right of ways and increase awareness of underground facilities in order to reduce the occurrences of back hoe fade.
NRIC VI-1C-09	Commercial Communications providers should consider developing service options that will deliver Calling Name and Number information to PSAP administrative lines regardless of the caller's originating privacy indicator. This option would allow PSAPs to identify potential emergency calls placed to their administrative lines during network re-routing, or other events that may cause the delivery of emergency calls to the PSAP's administrative lines. (ref. 5-569)
NRIC VI-1C-10	Coin phone service providers should make available a list of all Public Pay/Coin Phone locations within the service providers applicable territories for use by any requesting Public Safety entity. [for Rationale = In times of emergencies, Public Safety personnel could be able to locate and utilize public pay phones for essential communications if all other forms of communications are unavailable.]
NRIC VI-1C-11	Service Providers that offer Wireless PAS (Priority Access Services) should work with the NCS and the public safety community to promote the awareness of communication options currently available to those that qualify for the service in the Public Safety Sector.

Number	Proposed Recommendations to Issues Identified in Gap Analysis
NRIC VI-1C-12	This recommendation number not assigned.
NRIC VI-1C-13	This recommendation number not assigned.
NRIC VI-1C-14	Development of an equivalent to priority access services for public Internet access over CATV networks by Public Safety. (Reference BP 5-545).
NRIC VI-1C-15	When required by law, CATV providers should have procedures in place to support collection of information from caching servers and back-office systems for court orders or other appropriate reasons. (Reference BP 6-5-505)
NRIC VI-1C-16	CATV providers should have procedures in place to identify and respond to harmful actions or traffic being routed through their network. (Reference BP 6-5-505)
NRIC VI-1C-17	To ensure satellite service availability during an emergency, preparation and planning are critical. To this end, satellite carriers should work with Federal, state and local public safety agencies (including NCC) to ascertain requirements and availability of space segment capacity and assist public safety agencies in developing operational emergency procedures, including training personnel in how to expedite access to satellite facilities. Proper planning also encompasses provisioning and preparing ground terminals, both multiple user and individual user terminals, before an emergency, in order to gain satellite access quickly as well as integrating/interfacing satellite network operation centers with terrestrial facilities.
NRIC VI-1C-18	The process of “red tagging” circuits by Service Providers needs to be revisited by each provider to insure critical / essential circuits have appropriate “red tag” identification. “Critical” should be defined in context of national emergency / public safety.
NRIC VI-1C-19	To ensure satellite service availability during an emergency, preparation and planning are critical. The terrestrial network operation centers, the public safety operation centers, and the satellite operation centers, should hold pre-planning and coordination meetings to determine how they will coordinate if and when an emergency occurs.

Appendix H – Industry Role and Network Type Matrix

Each Best Practice (existing, modified by NRIC VI and Proposed by NRIC VI) can have associations with any combination of six industry roles:

- Service Providers
- Network Operators
- Equipment Suppliers
- Government
- Commercial Landlords
- Public Safety Services and Support Providers

The last three are new industry roles in NRIC VI, and the Public Safety Services and Support Providers was introduced for Public Safety.

This Appendix correlates the existing and edited (in NRIC VI) Best Practices that impact Public Safety to the Industry Roles (Service Provider, Network Operator, Equipment Supplier, Government, and Public Safety Services and Support organizations) and Network Type (Wireline, Wireless, Satellite, Cable, Internet).

Existing and Modified NRIC V Best Practices

No.	Service Provider	Network Operator	Equipment Supplier	Government	Commercial Landlord	Public Safety ervice and Support Provider	Wireline	Wireless	Satellite	Cable	Internet
6-5-505	1	1		1		1	1	1			1
6-6-509	1	1				1	1	1			
6-6-511	1	1	1			1	1	1			
6-6-512	1	1	1			1	1	1			
6-6-513	1	1	1			1					
6-5-522	1	1	1	1		1	1	1			
6-5-545	1	1	1	1		1	1	1			
6-5-646	1	1				1	1				
6-5-566	1	1				1	1				
6-5-566	1	1				1	1				
6-5-566	1	1				1	1				
6-5-566	1	1				1	1				
6-5-567	1	1				1	1				
6-5-568	1	1				1	1				
6-5-568	1	1				1	1				
6-5-569	1	1				1	1				
6-5-569	1	1				1		1			
6-5-570	1	1			1	1	1				
6-5-571	1	1				1	1				
6-5-572	1	1				1	1				
6-5-573	1	1				1	1				
6-5-574	1	1				1	1	1			
6-6-575	1	1	1			1	1	1			
6-5-576	1	1	1	1		1	1	1			
6-5-576a	1	1	1	1		1	1	1			

No.	Service Provider	Network Operator	Equipment Supplier	Government	Commercial Landlord	Public Safety Service and Support Provider	Wireline	Wireless	Satellite	Cable	Internet
6-6-577	1	1	1			1	1	1			
6-5-578	1	1		1		1	1	1			
6-5-579	1	1				1	1	1			
6-5-580	1	1		1	1	1	1	1			
6-5-580	1	1		1		1	1	1			
6-5-581	1	1	1			1	1	1			
6-5-584	1	1	1	1		1	1	1			1
6-6-586	1	1	1	1		1	1	1			1
6-5-598	1	1		1		1	1	1			1
6-6-599	1	1	1	1		1	1	1			
6-6-619	1	1				1	1				
6-6-655	1	1				1	1	1			
6-6-747	1	1		1		1	1	1			1
6-5-758	1	1	1			1	1	1			

This Appendix correlates the new Best Practices and Industry Recommendations that impact Public Safety to the Industry Roles (Service Provider, Network Operator, Equipment Supplier, Government, and Public Safety Services and Support organizations) and Network Type (Wireline, Wireless, Satellite, Cable, Internet).

Proposed New Best Practices

No.	Service Provider	Network Operator	Equipment Supplier	Government	Commercial Landlord	Public Safety Service and Support Provider	Wireline	Wireless	Satellite	Cable	Internet
BEST PRACTICES											
6-6-3201	1			1		1	1	1		1	1
6-6 3202	1	1		1		1	1	1			
6-6-3203	1					1	1	1			
6-6-3204	1			1		1	1	1			
6-6-3205	1	1		1		1	1	1	1	1	1
6-6-3206	1		1	1		1		1			
6-6-3207	1	1	1					1			
6-6-3208	1	1			1			1			
6-63209	1	1				1				1	
6-6-3210	1					1				1	

Appendix I – Priority Access Description

Why Wireless PAS?

Wireless telecommunications services are increasingly vital to the ability to coordinate and respond to crises. However, during emergency situations and natural or manmade disasters, and when wireline network outages occur, CMRS providers' wireless channels can become congested, thereby preventing NSEP personnel from obtaining access.

NSEP telecommunications services are critical to the maintenance of a state of readiness or the response to and management of any event or crisis that causes or could cause harm to the population, damage property, or threaten the security of the United States.

What is Wireless PAS?

Priority Access Service (PAS) provides a means for National Security and Emergency Preparedness (NSEP) telecommunications users to obtain priority access to available wireless radio channels when necessary to initiate emergency calls.

CMRS providers offering PAS will provide authorized NSEP personnel priority access to available wireless channels during emergency situations prior to any other CMRS users. Therefore, PAS helps to ensure that NSEP authorized personnel can complete critical calls in support of NSEP missions.

PAS enables NSEP personnel with a PAS assignment priority access to the next available wireless channel before subscribers who are not engaged in NSEP functions. Priority calls will not preempt calls in progress and PAS will not guarantee the completion of priority calls.

Service Providers

The Federal Communications Commission (FCC) issued a Report and Order on July 13, 2000, establishing the regulatory, administrative, and operational framework that enables commercial mobile radio service (CMRS) providers to offer PAS to NSEP personnel. CMRS providers include cellular licensees, broadband personal communications service (PCS) licensees, and specialized mobile radio (SMR) licensees.

The FCC rules do not require CMRS providers to offer PAS. Therefore, CMRS participation in the PAS Program is achieved on a voluntary basis.
Although the FCC maintains oversight responsibilities for the PAS Program, the National Communications System (NCS) manages the day-to-day administration.

NCS has said it would work with the wireless industry on a national solution by end of 2002 for initial operating capability (IOC) and would have full operating capability (FOC) by year-end 2003. FOC would provide 'end to end' priority service and interfaces with the rest of the Government Emergency Telecommunications Service known as GETS

(Wireline). Currently(October-2002), one CMRS provider offers limited PAS functionality in New York and Washington DC which provides outgoing/originating PAS service during periods of high congestion. By the end of 2002, it is expected that the same CMRS provider will deploy the limited PAS functionality for originating calls nationwide. Later other CMRS providers are expected to provide these services as well.

Users

Only personnel and individuals in national security and emergency response leadership positions may request PAS; PAS is not intended to be used by all emergency service personnel. The following PAS priority levels and qualifying criteria apply equally to all users and are used as a basis for all PAS assignments.

Priority 1: Executive Leadership and Policy Makers.

> Individuals in executive leadership and policy-making roles qualify for Priority 1 assignments. Examples include the President of the United States, the Secretary of Defense, selected military leaders, State governors, lieutenant governors, and cabinet-level officials responsible for public safety and health; mayors and county Commissioners; and a minimum number of senior staff to support these officials.

Priority 2: Disaster Response/Military Command and Control.

> Eligible for Priority 2 are personnel key to managing the initial response to an emergency at the local, State, regional, and Federal levels and personnel essential to continuity of government and national security functions. Examples include Federal emergency operation center coordinators and State emergency services directors.

Priority 3: Public Health, Safety, and Law Enforcement Command.

> Eligible for Priority 3 are individuals who direct operations critical to life, property, and maintenance of law and order immediately following an event. Examples include Federal law enforcement command and State police leadership, local fire and law enforcement command, emergency medical service leaders, search and rescue team leaders, and emergency communications coordinators.

Priority 4: Public Services/Utilities and Public Welfare.

> Eligible for Priority 4 are individuals responsible for managing not only public works and utility infrastructure damage assessment and restoration efforts, but also transportation services for emergency response activities. Examples include U.S. Army Corps of Engineers leadership; power, water and sewage, and telecommunications utilities; and transportation leadership.

Priority 5: Disaster Recovery.

Eligible for Priority 5 are individuals responsible for managing recovery operations after the initial response has been accomplished. These functions include managing medical resources such as supplies, personnel, or patients in medical facilities. Examples include medical recovery operations leadership, detailed damage assessment leadership, disaster shelter coordination and management, and critical Disaster Field Office (DFO) support personnel.

Appendix J – Nextel PAS Description

Beginning in February 2003, Nextel Communications and its network affiliate Nextel Partners (collectively, "Nextel") will offer the public safety community Dispatch Priority Access Service ("Dispatch PAS") for the Nextel service dispatch (push-to-talk) service – a voice service that, unlike cellular and other Commercial Mobile Radio Services, is not interconnected to the Public Switched Telephone Network ("PSTN"). This Dispatch PAS is available on the Nextel nationwide Integrated Digital Enhanced Network (iDEN). Dispatch PAS provides the user higher queuing in times of network congestion, increasing the speed and likelihood that Nextel Direct Connect® (one-to-one) and Group Connect (one-to-many) calls will be completed.

Nextel's Dispatch PAS provides for five levels of priority, based on the FCC Part 64 guidelines used by the NCS for GETS. Since priority is set at the network level, any handset (including legacy units) can be activated for the service (which is subject to a flat-fee monthly charge). The iDEN technology provides for protection from electronic eavesdropping on public safety communications, and dispatch calls do not enter the PSTN but instead are switched solely within Nextel's iDEN network. Nextel dispatch users today can reach any other subscriber across wide-area local service areas, whether within their "home" area or another local area while traveling throughout Nextel's nationwide network. By the end of 2003, priority dispatch will be available on a nationwide basis, so that public safety users can dispatch colleagues anywhere in the country. This technology is also available from Motorola, the network infrastructure manufacturer, for deployment by other iDEN carriers, although dispatch roaming across competing carrier networks has not been implemented. Priority service is not available at this time on interconnected calls over Nextel's iDEN network.

With nationwide dispatch, the Nextel priority dispatch system will provide a viable critical communications link during national, regional and local crises, and provides for seamless interoperability that can be implemented as a lower cost alternative to construction of new inter-agency private radio systems.

Appendix K – T Mobile PAS Description

T-Mobile USA has now been awarded the Nationwide Wireless Priority Service (WPS) contract by the National Communications System (NCS), through its WPS integration contractor DynCorp. Nationwide WPS is operational in a total of 15 metropolitan areas in the Eastern United States, with additional markets to follow. T-Mobile has been providing WPS in the greater Washington, D.C. and New York City metropolitan areas since May 2002

WPS enables designated national security and emergency preparedness (NSEP) personnel greatly improved capability to complete wireless calls during times of emergencies or natural disaster when wireless networks are stressed and overloaded.

When trying to make a call in times of emergency or natural disaster, WPS users have the ability to queue at the top for the next available radio resource from their closest base station in order to place their call, greatly enhancing their ability to complete wireless calls during these critical times and assist the situation. **WPS is available only to designated leadership** at all government levels, national security, emergency responders, and private sector critical infrastructure personnel, as approved by Federal Communications Commission Rules and Requirements and the National Communications System (NCS). The NCS is the only agency that can determine who gets WPS and assign the level (1 through 5) of priority.

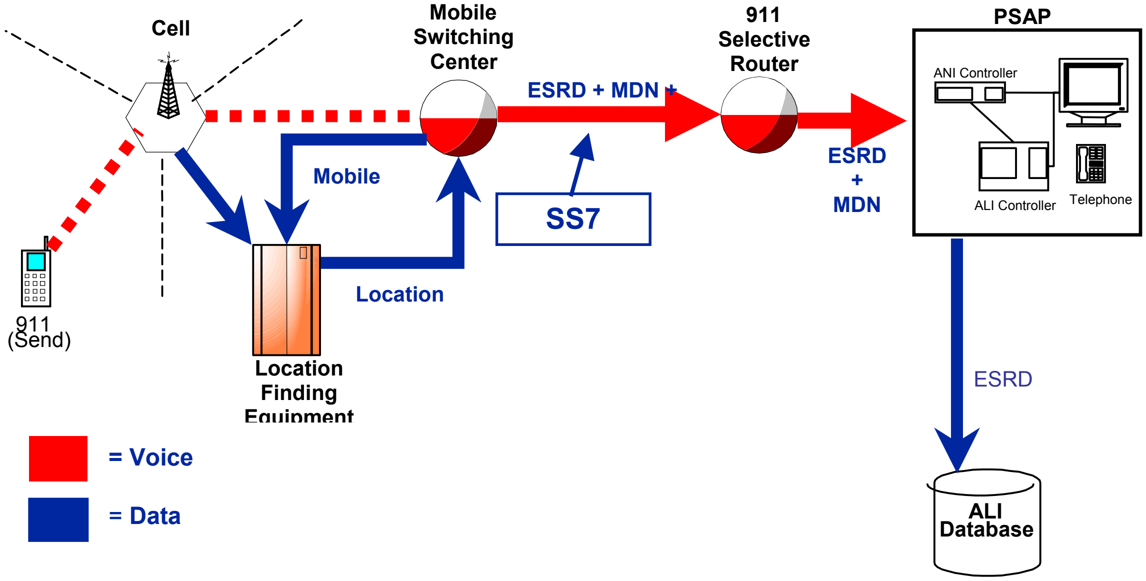
Additional details on the WPS program are available at: wps.ncs.gov or at 866 NCS-CALL.

About T-Mobile USA, Inc.

Based in Bellevue, Wash., T-Mobile USA, Inc. operates a nationwide GSM/GPRS voice and high-speed data network that covers more than 210 million people. T-Mobile USA is a member of the T-Mobile International group, the mobile telecommunications subsidiary of Deutsche Telekom (NYSE: DT). Additionally, T-Mobile operates the largest carrier owned 802.11b ‘Wi-Fi’ network in the country, under the name ‘T-Mobile HotSpot.’ T-Mobile is committed to providing the best value in wireless service through its GET MORE^{SM} promise to provide customers with more minutes, more features and more service than any other wireless provider.   For more information, visit the company web site at www.t-mobile.com.

Appendix L – Wireless E911 Phase I & II

E911 Phase I uses the ESRD (Emergency Services Routing Digit), a routable number within the North American Numbering Plan that represents the serving cell of the wireless caller. The ESRD is used by the Emergency Services Network to route the call to the appropriate PSAP (Public Safety Answering Point). The drawing below represents a wireless emergency call in Phase I.

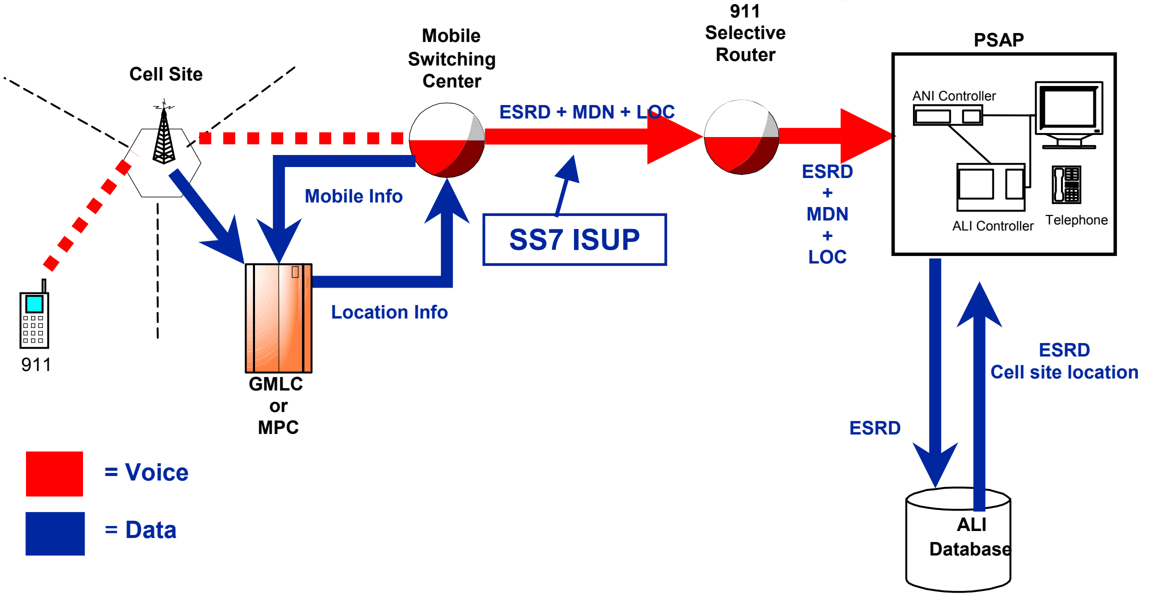


1. A wireless subscriber dials 911
2. The Cell transmits the call to the MSC
3. The MSC does a data base dip to determine the ESRD.
4. The MSC sends the call to the selective Router with the Mobile Directory Number (MDN) and the ESRD
5. The Selective Router determines what PSAP to route the call to based on the ESRD.
6. The Selective Router sends the call to the proper PSAP with the ESRD and MDN
7. The PSAP determines the Location based on the ESRD from the ALI database.

E911 Phase II mandates a wireless caller’s location (Lat. & Long.) is delivered to the PSAP with an accuracy of 125 meters 67% of the time. Two primary technologies have been used by different service providers to fulfill this requirement. One uses GPS (Global Positioning Satellite). This method requires a GPS device to be added to the cell phone and the callers Latitude and longitude are sent when an emergency call is placed. The other technology – triangulation, relies on the delay of the radio signal between three cell towers and the caller’s phone. This method needs no additional hardware in the cell phone. Both methods require a database GMLC (Global Mobile Location Center) or MPC (Mobile Positioning Center) for GPS and triangulation respectively.

There are two methods needed for delivery of the emergency call information to the PSAP, based on the interface between the Selective Router and the PSAP. The first is Call Path Associated signaling. The diagram below represents this method.

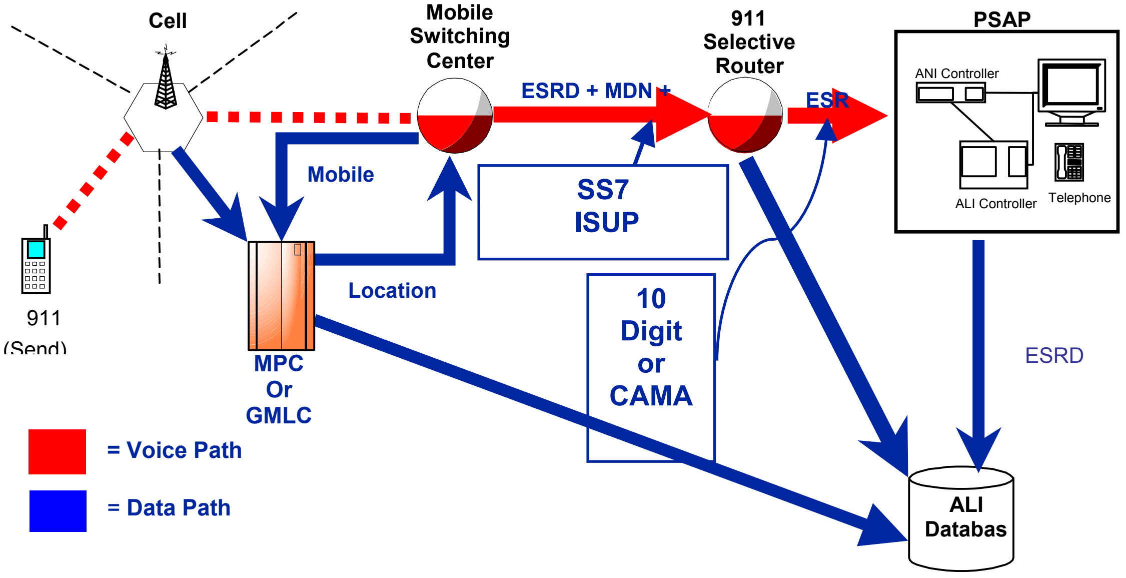
Call Path Associated Signaling



1. A wireless subscriber dials 911
2. The Cell transmits the call to the MSC
3. The cell phone transmits the GPS information or the three closest cells to the phone determine the time delay ; and this information is sent to the MSC
4. The MSC determines the Longitude and Latitude from either the GMLC or MPC database
5. The MSC sends the selective router the MDN, ESRD, and the Lat. & Long. Of the caller.
6. The Selective Router determines the Proper PSAP to route the call to and routes to it sending the MDN, ESRD, and Lat. & Long. Information.
7. The PSAP determines the location of the caller

The second method of delivering an emergency wireless call is non call-path associated signaling. The diagram below represents this method.

Non Call-Path Associated Signaling



1. A wireless subscriber dials 911
2. The Cell transmits the call to the MSC
3. The cell phone transmits the GPS information or the three closest cells to the phone determine the time delay ; and this information is sent to the MSC
4. The MSC determines the Longitude and Latitude from either the GMLC or MPC database
5. The MSC sends the selective router the MDN, ESRD, and the Lat. & Long. Of the caller.
6. The Selective Router determines the proper PSAP to route the call to and routes the call with the ESRD to the PSAP.
7. The Selective Router Sends the ESRD, MDN, & LOC information to the ALI database of the proper PSAP over a data channel.
8. The PSAP determines the location of the caller

There are three organizations that define the interfaces between the different network elements in an emergency call. They are:

- ATIS (Alliance for Telecommunications Industry Solutions) T1S1 - TI.113 ISUP
- NENA (National Emergency Number Association) – Wireless Subcommittee

TIA (Telecommunications Industry Association) TR45.2 – PN 3890 Ad Hoc for wireless service

Appendix M - Satellite Communications in Public Safety

Satellite communications provide a complimentary role to terrestrial wireless or wireline communication systems for Public Safety applications. Some unique features of communication satellite networks are as follows:

- National coverage with single network standard thus providing interoperability over a regional or national coverage area.
- Coverage of remote areas having little or no terrestrial communications facilities.
- Redirection of satellite capacity to any location in the country. Dynamic assignment of capacity as needed, including selection of time, frequency and location.
- Unique point-to-multipoint capability for broadcasting, conferencing or multicasting of information.
- Network Control Centers for Public Safety can be located at convenient locations nationally and directly monitor and control Public Safety services via satellite anywhere within the country.
- No dependence on terrestrial communications infrastructure.
- Same satellite can provide mobile communications to aircraft, ships, land vehicles and handheld terminals.

These features lead to the following use of communications satellites by the Public Safety community. The first, and most well know use of satellites, is the Wide Area Network (WAN) connection from the scene of an emergency situation by bringing to the scene transportable earth stations, either vehicle mounted or delivered in cases and quickly assembled at the emergency site. The earth station permits connection to a terrestrial network point of presence located anywhere in the U.S. This use of satellites bypasses the terrestrial infrastructure at the emergency location and permits satellite resources to dynamically be assigned to the given emergency site. Remote emerging sites may have to depend on satellite communications as their only means for WAN.

Another use of satellites in Public Safety applications is for surveillance and monitoring of critical facilities such as ports, energy and transportation assets, international borders, oil and gas facilities, etc. The satellite, because it has coverage over the entire U.S., can very easily monitor and control ground sensors located anywhere in the U.S., from one or more network control locations. Surveillance can also be provided directly from space using observation satellites (such as SPOT) with optical, infrared and other sensors on board the satellite.

As satellites are well suited for broadcast and multicast, relevant information can be immediately sent from an emergency site to key locations anywhere in the country, including informing the public on a given emergency.

One of the most important uses of satellites in the Public Safety application is individual user terminals, which can directly access the satellite. These terminals may be handheld terminals similar to cellular telephones, which are already in use on the following satellite systems: Iridium, Globalstar, and Thuraya. The user terminals can also be data terminals the size of a laptop, which can provide both voice and data services up to 400 KBPS. Most of the above terminals operate with Mobile Satellite Systems using the L or S band spectrum. It is also possible to provide direct user access terminals that operate with satellites using Ku- or Ka-band spectrum.