bile violations, such as expired licenses, expired automobile insurance, stolen vehicles and outstanding tickets.

- Their system allows access to three different sources for information: The Automobile License and Registry System (ALARS) which accesses registry information, the Law Enforcement Processing System, located at the State Police headquarters, allowing the officers access to outstanding arrest warrants and other information, and the National Crime Information Center (NCIC) for data on all out-of-state vehicles.

- With the new computers, an officer in a cruiser can get a response on the computer screen in 5 - 10 seconds, before he or she gets out of the cruiser.

- A silent dispatch feature allows for silent transmission between cruisers and the base unit at police headquarters, preventing anyone with a police radio from listening in.

- If an officer is driving behind a suspicious vehicle, the license plate is placed in the system, and a "reported stolen" message comes up on the screen, officers would call for help with the silent dispatch feature. Another cruiser or unmarked car would go to the scene and work its way in front of the vehicle. With a police car in front of the subject vehicle, at the appropriate, the lead car stops. This allows both police vehicles to box-in the reportedly stolen vehicle, eliminating a high speed chase and possible injury to officers.

This type of system is beneficial to departments that:

1) have a large number of units
2) need to patrol a large geographical area
3) are unable to dedicate a radio channel to data
4) who prefer not to operate their own data system
5) need to communicate among several departments within a county, city or town
6) need back up communications when normal circuits are interrupted

Secure calls

A third party vendor has received a "notice of allowance" by the US Patent and Trademark Office for an attachment to portable cellular phones that scrambles users' voices in order to secure call from unwanted monitoring or eavesdropping. The device is an electronic extension system for a portable cellular phone that does not require any modification to the phone for use. It slides between the phone and its battery. It is electronically connected to the phone through a specially designed floating connector that plugs into the peripheral port of the phone. The extension uses electronics that are independent from the phone's speaker and microphone to provide voice capabilities.

ANI/ALI Integration

Nearly all public safety dispatch centers are equipped to accept 911 emergency calls. In it's basic form, a 911 system captures the calling party's telephone number, and displays it to the dispatcher. In enhanced versions, the telephone number is cross-referenced to an address file and the calling party's street address is also displayed.

Some dispatch centers are equipped with Computer Aided Dispatch (CAD) systems that can take this a step further. CAD systems are typically developed by third-party vendors. Most of them cross-reference files with other important information such as number of prior disturbances or calls to a location, presence of hazardous materials at the location, etc.

Developers could program CAD software to forward this information to public safety representatives carrying portable devices. The information would arrive in a text message format supported by most commercial wireless data vendors.

g) E-mail support

Popular third-party e-mail vendors have supported messaging across a wide variety of wireless carriers. Today, many wireless carriers will accommodate e-mail data traffic. That means that an e-mail message generated on a remote wireless device could be received by another portable device on a different type of network.

An example would be an e-mail message originated on an SMR network and received on a pager. In a public safety environment, e-mail transmission would be most suitable for non-critical communications, like transmission of reports, notification of meetings, etc.

h) Third-party product information

Public safety organizations such as the Association of Public-safety Communications Officials (APCO), and Public Safety publications such as the Public Safety Product News, make third-party value-added products and services information available to public safety agencies. APCO publishes an annual Communications Buyer's Guide which lists public safety products and suppliers.

i) Internet support

Internet addressing is another way for wireless providers to send messages across disparate networks. As with e-mail, in the public safety environment, Internet messages would be most suitable for non-critical, non-secure communications like notification of meetings, etc.

j) Public Switched Telephone Network (PSTN)

According to a representative from the New York State Police, "So far, access to the PSTN, as a mechanism for interoperability between individual users of different systems and between individual members of a group with no other common system, have been described. In these modes, the common denominator has been the PSTN, where standards already exist to ensure that different systems can communicate with each other".

Satellite, paging, cellular and PCS commercial services interoperate through the public switch.

Satellite, systems have a particular advantage regarding PSTN connectivity when terrestrial systems are stressed. Their access to the PSTN is via a distant gateway station unlikely to be affected by a localized or even wide spread emergency.

12.9.4.2 Future interoperability

a) Planned networks

Interoperability is a key component of emerging Low Earth Orbit technology. When a call is made from the satellite handset, the handset first searches for a local cellular network. If one is found, the phone will function as a normal cellular telephone and the call will be routed along standard cellular paths. If no cellular network is found, the handset becomes a satellite transceiver. It makes contact with one of the satellites which then routes the call through the satellite/gateway constellation. The signal passes from satellite to satellite until the call is sent to the appropriate gateway, nearest to the call's destination, where it is then transferred into the public switched telephone network.

Additionally, LEO representatives now believe it is possible through their relationship with manufacturers to adapt private land mobile radio equipment to interface to LEO networks in addition to cellular. The introduction of those interface services will depend on market demand.

12.9.4.3 Commercial Wireless Interoperability Initiatives

Not unlike the market forces that are creating wireline interoperability at multiple levels on the Internet, commercial providers portend that market conditions will encourage the same level of interoperability in the wireless world.

To that end, commercial initiatives have begun to focus at minimum, on gateway technology that will allow vendors to transfer short data messages at a basic level of service across disparate networks. Where standards are needed to achieve ubiquitous user interface for emergency services, vendors are voluntarily participating in working groups to explore solutions.

Examples of some of those initiatives would include:

1) The Satellite Communications Division of the Telecommunications Industry Association (TIA) to address Communications and Interoperability.

The Satellite Communications Division of TIA had it's first meeting on January 17, 1996, and was attended by 48 representatives of the satellite industry from over 25 companies and government agencies. A Communications and Interoperability Section was formed.

The first meeting of the Communications and Interoperability Section of the Satellite Communications Division was held on March 20. The mission of the group was defined.

The mission states:

The mission of the Communications & Interoperability Section is to address issues that affect the continued development of the satellite industry. These issues include and are not limited to:

(1) *Identification of technical issues relevant to Global Communications which need to be investigated for interoperability*

(2) *Investigation of high level hybrid reference models within the context of interoperability*

(3) *Development of detailed contributions and position papers proposing possible solutions for interoperability*

(4) *Modification of existing standards and develop new standards and advocate their adoption in national and international standards bodies*

(5) *Consideration of experiments to test interoperability and validation of the protocols and standards"*

2) The Commercial Mobile Satellite Systems (CMSS) Working Group of the Interagency Committee on Search and Rescue, was created to address how mobile satellite services can support remote area distress alerting and locating, including first response operations support of search and rescue.

The CMSS Group has representation from all the major mobile satellite communication system suppliers (existing and planned), and most of the government agencies concerned including: DOT (USCG & FAA), DOD (USAF), NOAA (NESDIS), FEMA, DOI (NPS), FCC & NASA.

This government-industry task group was formed to review the issues involved in distress alerting and locating using mobile satellite systems. Standard user interfaces, alert routing, common PSTN/PSDN interfaces, priority access and other desirable features are issues explored.

3) Focus Group IV of the Network Reliability Council was asked to focus on how effectively new technologies, e.g., commercial mobile radio services (CMRS) or cable television, can back-up existing essential communications networks such as 9-1-1. The Focus Group, for purposes of the following report, is referred to as the Essential Communications During Emergencies (ECOMM) Team.

Early this year, their report was produced, entitled, Network Reliability Council Focus Group IV. Essential Communications During Emergencies Team Report. Findings and Recommendations, dated January 12, 1996.

That document stated, It is important to understand how current and future networks that rely upon new technologies, e.g., commercial mobile radio services (CMRS) or cable television, can back-up existing essential communications networks such as 9-1-1. Focus Group IV of the Network Reliability Council (NRC) was asked to focus on how effectively these new services can augment and/or replace essential emergency communications networks that may be unavailable in case of a network outage.

4) Regional consortia of agencies such as the Washington-Baltimore High Intensity Drug Trafficking Area (HIDTA) and the Local Government Information System (LOGIS) in Minnesota are conducting research of the potential application of commercial wireless to their operations.

12.9.5 Commercial Coverage Options

Often, lack of coverage availability is confused with lack of network reliability. Knowing which commercial service vendors provide coverage throughout the geography users most frequently travel is a major key to the successful use of commercial services. It is also important to understand how network and device characteristics vary. Providers have different strengths and weaknesses depending on the environment.

12.9.5.1 Remote locations

Terrestrial-based systems are expensive to build and maintain in sparsely populated locations. Unless provisions have been made for portable terrestrial systems to be furnished for specific requirements, a more suitable means of communications is more likely to be satellite. Since satellite communications rely on line-of-site, indoor applications will require other options.

Marine-based and remote disaster relief operations are best served by satellite systems. Wildfires, agricultural, environmental (hazardous spills) and weather related applications

require non-terrestrial based systems. Although use of such links have typically been limited to administrative and logistical support, recently introduced technologies and equipment may lend to increased utilization.

Other applications include remote surveillance and border patrol activities.

Small towns often have local cellular, SMR and/or paging vendors that operate within a well-defined footprint around the population center. Public safety providers may find it necessary to understand how well local vendors interoperate with vendors outside of those immediate footprints should an incident occur requiring remote, interjurisdictional or interdisciplinary support.

12.9.5.2 Urban locations

Cellular, PCS, paging and SMR terrestrial infrastructures are more densely concentrated in the heavy population centers around major cities. Generally, carriers in the higher MHz frequency range are more successful with applications requiring in-building penetration, although system design may not be intended for the in-building coverage required public safety. These services, though generally available above ground, may not be available below ground as in subways and tunnels.

12.9.6 Public Safety Issues That Impact the Use of Commercial Wireless Services

12.9.6.1 Planning

Command/Control

Some commercial wireless services could be effectively incorporated into command/control procedures for mutual aid if those procedures are written to include the use of commercial services. Clearly outlined communication protocol based on identified resources would help providers understand their role.

Using commercial-off-the-shelf (COTS) products and services, with limited R&D it is feasible to develop an electronic switching matrix that will have the capability to provide full crossband, multi-code, secure to non-secure RF communications. It would require cooperation between local, county, state and federal agencies and the commercial sector. This system could be developed by a cooperative venture between the commercial and public sector. It could provide cross connects to satellite links, local telephone interconnect and microwave relay stations if necessary. Planning and communicating with each of the participating agencies and commercial sector companies would be essential to the success of such a project.

Today bottlenecks often occur because Public Safety agencies may not identify what commercial wireless communications options exist prior to an actual event. In addition, the application of appropriate wireless communication tools based on

protocol, procedure and the environment setting where the event occurred, may not be defined.

The Metropolitan Washington Area Interoperability case study (refer to document #PSWAC/ISC 96-04-024/2 at Appendix C) about the Fourteenth Street Bridge disaster which occurred on January 13, 1982, outlines deficiencies in available wireless communication resources. Additionally, per the study, subsequent efforts to address communication needs via a formal Mutual Aid Plan have still not satisfied requirements. On page 11, MAP participants list communication difficulties they have continued to experience in responding to other disaster situations.

The lack of a clear command/control organization from the onset of an event, makes it difficult for well-intentioned commercial vendors to provide assistance.

On May 11th, 1996, ValueJet flight #592 crashed in the Florida everglades. According to sources called to the scene, 30 hours elapsed before a formal command/control center was established by the National Safety Transportation Board. In the meantime, three quasi-command posts/staging areas were established. They were:

1) an EMS staging site/command post at the Opa-Locka airport
2) a Dade County police staging site/command post on the Tamiami Trail
3) a Dade County fire department staging site/command post on a service road along the L 67 canal

Additionally the FAA established a level of command from the Miami airport.

Apparently media coverage of the disaster varied, depending on which command site they were quoting.

In this particular incident:

1) *Were the command posts in communication with one another?*
2) *Which command post was taking the lead to provide cross jurisdictional, cross agency wireless communications?*
3) *If a commercial wireless provider were willing to offer assistance, who would they contact?*

Under these types of circumstances, the role commercial services can play in mutual aid, joint or task force operations gets lost. In the future, if emergency preparedness plans include the use of commercial services, commercial providers can play key roles in supplementing existing communication capabilities.

Dade County Officials could have incorporated the use of commercial satellite services, or potentially portable PCS, cellular or paging services in a Mutual Aid Plan prior to the crash. That way, rapid deployment of communication terminals,

PCS/cellular phones, or paging devices on a single or interoperable commercial frequency(ies) from designated emergency preparedness locations could have helped designated authorities make faster, more collaborative decisions, and establish levels of command quickly. Even with the deployment of a portable cell site, there does need to be a way to connect that cell site from the remote location into the provider's infrastructure, typically a micrwave link, or links, will be required.

Wireless data updates to handheld satellite terminals or alpha pagers from a central dispatch point, could have kept media stories straight.

Information about the arrival and location of Salvation Army representatives who provided food and beverage, could have been quickly shared and updated with rescue and staging personnel. According to workers, dehydration was a serious concern for workers. It was difficult to work more than fifteen minutes at a stretch without liquids due to the extreme heat. Although this operation was initially characterized as a rescue operation the designation quickly progressed to a retrieval operation as it became apparent that there were no survivors.

Under those circumstances, life threatening decisions are not eminent, but operations will continue. Commercial wireless services can fulfill a major role in providing alternate communication resources in order to free up existing private radio spectrum for other use.

ECOMM findings

Network Reliability Council Focus Group IV. Essential Communications During Emergencies Team Report. Findings and Recommendations. dated January 12, 1996.

The Focus Group, for purposes of their report, is referred to as the Essential Communications During Emergencies (ECOMM) Team.

Their report states: The cellular industry handles over 18,000 call daily to 9-1-1. Routing and identification of wireless callers are considered significant problems for emergency service providers.

a) Recommendations included:

1) *CMRS (commercial mobile radio services), and cable television operators should develop, in partnership with the PSAPs (public safety answering points), work plans to support essential communications during emergencies.* (pg 3)

2) *Network service providers, 9-1-1 administrators, and public safety agencies should continually strive to improve communications among themselves. They should routinely team to develop, review and update*

disaster recovery plans for 9-1-1 disruption contingencies, share information about network and system reliability and determine user preferences for call overflow routing conditions. (pg. 52)

3) *Contingency plan development is the process of planning for recovery from a disaster that could impact the critical functions of a business operation. In broad terms, disaster recovery planning involves the following elements*:

- Advance planning and arrangements necessary to ensure continuity of critical business functions.

- Making sufficient agreed-upon preparations and designing and implementing a sufficient set of agreed-upon procedures for responding to a disaster event.

- Developing a plan which covers events that could result in the total or partial loss of operational capability or destruction of a physical facility.

- Developing a plan which includes procedures and availability of critical equipment and personnel for both automated and manual functions.

The service provider (i.e., LEC, ATP, or CATV) has the responsibility to ensure continuity of service to the PSAP in the event of a disaster impacting their service delivering networks.

Some alternate technology providers have supplied their critical employees with portable computers, equipped with high speed modems, for them to remotely access switches. Critical employees are expected to work from a location that allows them access to the switches during times of emergencies/disasters.

Most alternate technology providers do not have a formal plan on where employees are to report for work if their primary work place is inaccessible, for whatever reason. Some alternate technology providers have indicated they are investigating this issue and that they intend to develop plans in the future.

PSAP administrators have responsibility for developing a plan to ensure continuity of 9-1-1 service in the event of a disaster which impairs the functionality of a PSAP. In so doing, PSAP administrators must evaluate and plan for response to a range of risks to PSAP functionality, including but not limited to:

- Loss of commercial power
- Physical damage to the PSAP (natural or man-made disasters), including fire, earthquakes, etc. (pg 48)

- System software and hardware failures
- Communications link failures (network redundancy and diversity issues).
- PSAP center evacuation and relocation of personnel.

With the current availability of alternate technologies, PSAP Administrators should more aggressively pursue use of these technologies during wireline network failures. However, it is critical that the alternative providers support and implement Enhanced 9-1-1 features equivalent to wireline ANI and ALI service.

Wireline and wireless network providers should develop response capabilities to meet communications demands during large-scale emergencies/disasters. Plans should include, as a minimum, such topics as mutual aid agreements, NSEP issues, contact lists, and locations of critical equipment. (pg 49)

Steps toward planning commercial service interoperability

The success of commercial services in the public safety market will depend on how well they are assimilated by public safety agencies into application environments. Planning the intended use of commercial services for specific purposes is essential. When a major event occurs without planning, circumstances make it difficult for providers to offer effective service.

In some cases:

1) providers may not have plans of their own to support public safety applications
2) providers may have plans to support public safety applications that fall short of requirements
3) circumstances may have changed a provider's capability to support public safety requirements

Steps that would optimize the use of commercial wireless services in the Public Safety environment would include agency initiated action to:

1) identify requirements that lend themselves to commercial provider services
2) identify commercial services that may meet some of their requirements
3) test potential commercial services prior to an actual event
4) stay current on newly introduced technologies
5) use (commercial-off-the-shelf) COTS services when it makes sense to keep costs in check
6) use providers in applications that capitalize on their strengths
7) always have primary and alternate commercial providers in queue when available
8) look for providers that have open architectures for interoperability
9) make certain providers understand each application's requirements (take them on a field trip)

10) develop detailed implementation plans for commercial services

The more agencies provide vendors with clear expectations about when and where they plan to use commercial services, the more likely they will get the information they need to determine whether a vendor can meet their coverage requirements.

A recommendation that addresses planning procedures for interoperability was submitted to Working Group #9 by a Research Firm which specializes in public safety. The recommendation, originally intended for a regional law enforcement effort, suggests that an interoperability manual be constructed containing critical communications parameters of each of the participating jurisdictions and supporting agencies which may be called upon to support operations conducted by the lead agencies. Please see attachment A.

12.9.6.2 Public Safety Awareness of Commercial Wireless Services

Careful evaluation of commercial wireless services will require agencies to analyze a broad range of issues.

Commercial wireless communications providers have different standard operating procedures (SOPs) from one another. Each vendor's SOPs may reflect different response times, mean-time-between-failure (MTBF) statistics, service and repair procedures including escalation and troubleshooting, relationships with their support vendors, acceptable quality of service and security procedures. As with all products and services (as well as private public safety network providers), some vendors simply do a better job than others in some or all of those areas.

Public safety agencies need to clearly and realistically assess which applications are appropriate for commercial service support, and define the requirements for those applications clearly and realistically to potential vendors.

Distinctions should be made between providers, based on evaluations and pilot tests. Acceptable models and methodologies for comparison should be developed to compare all wireless service offerings, including in-house capabilities for optimal results. Models and methodologies need to be flexible enough to consider requirements for each application individually. Application requirements may differ significantly based on urgency, priority, geography, interoperability, security, immediate environment (on foot, in autos, in buildings, in remote or urban settings, etc.), length of message, need for history logs, etc.

If there are special circumstances that require a customized service not available in the commercial marketplace, agencies should consider the cost of developing and maintaining a custom solution in-house verses the costs associated with managing a third-party relationship for the development and maintenance of the same.

If an agency chooses commercial solutions for some applications, then it is up to the agency to develop the expertise necessary to manage a third party relationship effectively. Skillsets needed for successful program/project management may differ considerably from existing skillsets acquired to manage/operate and in-house network.

Some local agencies are not large enough to have a technical telecommunications staff capable of conducting independent research and technical evaluation. Contract officers who may, or may not have a technical background, look to vendor representatives as sources of technical information. Acquisitions of systems resulting from this process may not fully consider system performance, ease of integration and scalability.

Studies regarding public safety familiarity with commercial wireless service capabilities and their current role in public safety are not encouraging. According to a study conducted for The Maryland State Police of police departments throughout the country. Although police identified many problems with their telecommunications systems, they were unable to express high levels of knowledge of current and future systems. They were unable to identify sources of knowledge for telecommunications information other than vendors and other police units[18].

One state-wide research effort of all law enforcement organizations in the state showed less than two percent of the agencies were aware of the impending arrival of numerous space based telecommunications systems. Low levels of knowledge of current and impending technology combined with a tendency to use other public service agencies as a primary source of reliable information on communications systems.

Data bases of commercial firms products, capabilities, limitations, and current customers exist in a few, primarily large, jurisdictions. In some of these, the officers responsible for the development of requirements, requests for proposals, requests for quotes and the like are denied access to the data base for fear of impropriety or favoritism, the data base being used only by contractual personnel. In other locations where data bases do not exist, and the organizations are not large enough to have a technical telecommunications staff capable of conducting independent research, non-technical officers often resort to vendor representatives with a vested interest or to fellow officers in other organizations (who are also usually not technically qualified) as sources of information. Acquisitions of systems resulting from this process thus tend to be influenced by marketing hype rather than performance in relationship to performance requirements or by performance results in other organizations whose operating environment may not be similar to the acquiring organization.

The initial acceptance of commercial wireless services as a viable alternative to private systems will depend on the context in which they are employed.

---

18 pg 23 , Maryland Law Enforcement Telecommunications Interoperability Analysis, Focused Research, Oct. 93.

Recognizing the strengths and limitations of commercial services will be the first step toward applying them to achieve the most effective results.

Efforts to increase public safety awareness of commercial wireless services could conceivably include a variety of approaches. One such approach has proven effective in an industry that has experienced comparable challenges.

The health care industry has experienced paradigm shifts similar to public safety communications. The consolidation of private healthcare providers into a managed care environment in some ways parallels the move towards national interoperability in public safety communications. In both cases, a lack of resource and solidarity has resulted in serious introspection of business as usual, and intense exploration of alternative approaches.

The healthcare industry is slightly ahead of the public safety communications in experiencing the effects of their consolidation (verses standardization).

As a result, one can find no shortage of industry briefings, seminars, educational forums, etc. geared for every level of professional in the healthcare industry. These symposia are sponsored by healthcare associations, managed healthcare organizations, academia, industry experts, etc. An entire industry has emerged to address the issues associated with the changes in health care. It is still early in the change cycle for public safety communications, but programs are beginning to surface.

Two major Universities, the University of Maryland in College Park, MD and the University of Massachusetts in Lowell, MA are developing unique approaches that address these needs. Maryland's approach is a for credit, multi-disciplinary masters curriculum for law enforcement that includes a technology sequence teamed with small and large business.

Massachusetts is considering a series of continuing education courses for public safety which would include a similar team approach. Teams made up of academic, federal labs, and business would provide intensive insights into the technologies selected for study. Proceedings of these courses could be converted to CD-ROM for retention by those attending.

Undergraduate courses such as the intelligence analysis curriculum at Mercyhurst College in Pennsylvania have the potential of developing research staff for public service organizations which lack a research capability, but nationwide expansion of similar courses would be needed to provide an adequate base in reasonable time.

The next step academia must consider is how to link educational activities to communications goals through practical application.

Academia will attract an audience interested in exploring alternative approaches to wireless communications assessment.

Firms with telecommunications products and services can sponsor forums to meet with public service organizations wherein the public service organization users communicate with TECHNICAL staff of the companies relative to their operational environments.

Federal technology transfer symposia attract public service representatives. However, they are often heavily represented by federal laboratories and participating consultants. In many cases, the concepts presented are quite developmental in nature. With limited financial resources, public safety agencies often choose not to invest in immature technologies unless supported by demonstration grants. Further, systems highlighted as being available for transfer from DoD and other federal research are often cost prohibitive to the small and medium sized organizations that make up the vast majority of the public service community.

Commercial technology expositions and symposia often attract attendance by public service organizations but result in little progress. The current tendency to large trade shows dominated by marketing efforts does not provide the learning environment needed to provide public safety officials with the awareness and background to make adequate decisions. Marketing personnel at trade shows do not always include balanced discussions that address the limitations of their products.

Only if public service organizations, industry, and academia combine their efforts in consortia, partnerships and demonstration projects will the current multi-disciplinary shortfalls be overcome. Manufacturers and Commercial Service Providers desiring to present and field test new products, can demonstrate those products more readily by providing shared financing with the public safety agencies to do so.

12.9.6.3 Commercial Wireless Service Providers' Awareness of Public Safety

Firms introducing new wireless telecommunication products are often not experienced in marketing to the public service community and may not be aware of the potential application of their products and services to public service.

Firms need encouragement to conduct technical research and development that includes potential application to public service employment of their products. Research programs in both industry and academia could establish industrial internships wherein employees serve in public service organizations to learn the overall environment of specialized organizations.

Most vendors are very concerned about doing the right thing when it comes to public safety. They have been looking to the public safety community for guidance.

Vendors are anxious to learn what services they can provide that would prove acceptable in the public safety environment.

12.9.6.4 Third-party firms specializing in commercial wireless and/or public safety communications

Third party companies offering research, assessment and consulting services with experience in public safety communications are beginning to appear. Third parties are often able to offer an unbiased assessment of current and planned communications technologies. Some also operate as information brokerage firms using global access to on-line information to support their analyses.

Other information service companies provide subscriptions that can provide agencies with access to information regarding emerging wireless technologies on CD-ROMs. Areas that they claim to address include:

1) How wireless communications is defined and ways it can be used.
2) Whether commercial wireless networks and wireless data communications are economically feasible. alternatives to building and maintaining networks.
3) What products are available for wireless data communications and what technologies are available.
4) Vertical applications for wireless computing.
5) Comparisons between PDAs and notebook computers.
6) The market status of PDAs and pagers.
7) Narrowband PCS paging, its technologies, applications, market status and products.
8) Applications for wireless telecommunications
9) Standards and technologies.
10) Cellular technology.
11) Selection of wireless service providers.

12.9.6.5 Network Availability/Priority Access

The need for commercial service providers to support priority access has been recognized as a key issue during the PSWAC process. However, priority access should be considered one component of overall network availability to deliver information. The ability for service providers to deliver information reliably while meeting public safety response time and throughput needs requires end-to-end service and support.

Even if commercial providers comply with priority access practices in order to deliver messages to the public switch, accurate and timely routing and handling of those messages from the switch to the end office is necessary to guarantee successful delivery. Priority designations are lost when communications enter the Public Switched Networks as they are currently configured, unless dedicated lines are provided between gateway stations and public service agencies.

The findings of the Network Reliability Council Focus Group IV, document number ISCWG9047, emphasizes the importance of Public Safety Answering Point (PSAP) wireline backup (pg 41), and hot site back-up contingency plans (pg. 48).

In order to achieve priority throughput, calls through the PSAP, cannot be interrupted by (PSAP) facility incapacity. According to the study, "To accommodate instances where these facilities are interrupted or it becomes necessary to evacuate the PSAP location, some PSAPs have established mobile PSAP systems that may be connected to phone jacks at the serving end office. The phone jacks, although usually installed inside the end office for security purposes, are typically installed in an accessible location for ease in locating them during an emergency.

Some PSAPs have prearranged with the serving LEC to permit a jurisdictional employee having an emergency vehicle (e.g., police car) equipped with radio capability to retain a key to the LECs end office and to connect to an RJ-11 jack for 9-1-1 call interception. (pg 41)

It may also be possible to bypass wireline outages by using a cellular-to-cellular link within a cell site or through a cellular network infrastructure. The New Jersey State Police uses cellular bypass of failed tandem circuits in their E9-1-1 systems.

Surprisingly, fewer than 50% (of PSAPs) have current plans for what they would do during a network failure. (pg 30)

Separately, commercial priority access compliance loses significance if the commercial network fails to meet reliability criteria. Lack of redundancy can produce weak links even if traffic is carried on a "first-in, first-out" basis. First-in, first-out becomes meaningless should a vital network component go down with no backup.

Some commercial systems are being designed to provide several levels of priority access. Public safety organizations will need to establish procedures for their use. This emphasizes a need for a national focus on operational procedures, standards for systems, training and interoperability.

Priority access procedures have been outlined by marine and aeronautical agencies for satellite services. Cellular service priority access issues are currently being addressed in the Cellular Priority Access Service Subgroup (CPAS) of the Wireless Services Task Force, National Security Telecommunications Advisory Committee.

Details regarding CPAS as outlined by a representative of the CTIA follow:

Situation Analysis

Wireless telephone systems are typically designed to a 0.02 grade of service or better. This means that, during the system's peak busy hour (any one-hour interval during a

24-hour period during which overall call volume is at its highest), callers attempting to place a call over the wireless system have a 2% or less probability of being unable to complete the call due to the unavailability of a radio circuit. A user attempting to call during a period when all channels are busy will receive a reorder tone, more commonly known as the fast busy. By the time the caller re-attempts the calls, the strong probability is that a channel will be available. The traffic engineers for wireless telephone systems strive to strike an optimal and economically-sound balance between average traffic demands and peak traffic demands. The inconvenience of having to place a call again during times of peak system busy is offset by the lower overall expense associated with using the system.

A familiar example will help to illustrate this point. If Interstate 95 were built to handle all vehicular traffic presented on the Wednesday night before Thanksgiving, it would be 14 lanes wide in each direction. During the rest of the year, however, most of the capacity would be idle, representing a waste of the taxpayers' money. Motorists traveling at peak travel times experience delays on the highways, just as callers calling during peak traffic times on wireless systems experience delays.

During periods of emergency, traffic on wireless networks increases significantly for a variety of reasons. First, there is diversion of traffic from wireline to wireless systems. In the case of natural disasters such as hurricanes and earthquakes, the wireless systems may continue to operate even though overhead phone lines have been severed. Calls that would otherwise have been placed over the wireline network migrate under these circumstances to the wireless network. Second is a sharp increase in overall calling volume, as citizens affected by the natural disaster call to seek relief, to notify family members, to report emergencies and the like. Third is the increased call volume from the mass media covering the disaster and the corresponding relief efforts. Fourth is the increased use of wireless networks by the public safety agencies engaged in responding to the disaster. These conditions can develop on an area-wide basis, as is the case with hurricanes and earthquakes, or they can develop on highly localized basis as is the case with airplane crashes or train wrecks. When emergencies develop, the sharp increase in call volume taxes the system beyond its capacity, either system-wide in the case of regional disasters or site-specific in the case of localized disasters.

The public safety agencies seek to gain priority access to the wireless networks, so that telephone traffic associated with emergency relief efforts can take precedence over all other utilization of the system.

It is important to note the distinction between having priority access to a particular network and having assurance of call completion. Wireless carriers control only the access to the wireless portion of a telephone call's path. In times of emergency, a radio channel may be available, only to have the call blocked due to unavailability of long distance circuits or central office facilities. In the simplest analysis, wireless carriers obviously can exert no control over whether a user receives

a busy signal because the dialed number is already in use. This same admonition applies to other components of the telephone network as taken in its entirety.

Regulatory Issues

Regulatory and eligibility issues are being addressed at the national level by the National Security Telecommunications Advisory Committee (NSTAC). In partnership with NSTAC, the Office of the Manager, National Communications Commissions System, is seeking the FCC's approval to establish Cellular Priority Access Service (CPAS). CPAS will offer non-preemptive priority queuing cellular service to the nation's emergency responders who have national security or emergency preparedness functions.

To invoke CPAS, users must have a bona fide National Security or Emergency Preparedness purpose. Their telecommunications are used to maintain a state of readiness or to respond to and manage any event or crisis which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the National Security Emergency Preparedness of the United States. The proposal urges the creation of a centralized administration within one Federal Government office, to ensure uniform application of eligibility, procedures and rules and to provide a single point of contact for information and problem resolution.

CPAS defines 5 priority levels and supports the activities of both the private and public sectors. A petition for rulemaking was filed with the FCC by the National Communications System on October 19, 1995, recommending that CPAS be a voluntary service offered by the nation's wireless service providers.

Technology Issues

The technical issues associated with implementing a priority access system appear to be manageable. The architecture of all wireless telephone networks includes a signaling component which operates discretely from the actual service channels. Thus, even when all of a cell site's voice channels are occupied, the signaling channel is still processing requests for channels.

Historically, the Advanced Mobile Phone Service (AMPS) specifications identified a field in the Number Assignment Module (NAM) of the subscriber equipment called Access Overload Class (ACCOLC). Valid values for the ACCOLC range from 00 to 15. During provisioning of the subscriber unit, the value entered in the ACCOLC field was typically zero followed by the last digit of the subscriber's telephone number, or more accurately the Mobile Identification Number (MIN). During times of traffic overload, it was originally contemplated that cellular carriers could invoke a rolling "brownout" by denying system access to all ACCOLC values of 00 for, say, ten minutes, then all 01 values for the next ten minutes, and so forth until call attempts fell back within system traffic design limits.

This implementation of ACCOLC left available the higher values from 10 through 15 for assignment as priority units. Such an implementation would have permitted cellular operators to deny service to all values of ACCOLC below 09 during extreme conditions. However, no systems in operation today are known to have implemented full Access Overload Class operations.

More recently, the cellular industry has defined a service called Priority Access and Channel Assignment (PACA), which allows a subscriber to have priority access to voice or traffic channels on call origination. As described in TIA/EIA SP-3545, this feature permits a subscriber to obtain priority access by queuing eligible subscribers' originating calls when channels are not available. When a channel becomes available, the queued subscriber is served on a first-in-first-out basis.

Subscribers are assigned one of n priority levels at subscription time (where n has a minimum of eight and a maximum of fifteen). Priority levels are defined as 1,2,3,...n, with 1 being the highest priority level and n being the lowest priority level.

The invocation of PACA is determined by subscription to one of two options: Permanent or Demand.

- In the Permanent option the feature is always available and is used automatically whenever the subscriber attempts to originate a call.

*- In the Demand option the feature is available only on request. The subscriber requests PACA by using a feature code with an origination request. To invoke priority access, callers would enter a string of digits such as *44. The mobile switching center would recognize the mobile unit as having priority access, and could move the call to the front of the queue. This feature could be modified to offer priority on a per-call basis (requiring the user to enter the feature code on each call for which priority access is desired) or on a set interval basis (which would maintain priority access for a predetermined interval such as 4 hours). This switch-based approach works universally with any subscriber unit.*

Security

Implementation of priority access would require security measures to ensure that only authorized agencies can avail themselves of the priority access.

During the early development of the cellular industry, programming the NAM required expensive special equipment and considerable technological acumen. All cellular units today, however, can be programmed through the handset of the phone. This creates a security issue in that subscribers not authorized for priority access could nonetheless program their own ACCOLC to the higher values. A feature-code approach would be similarly vulnerable to compromise.

Universality

Disaster relief often brings specialized teams in from distant areas. Any priority access scheme must be nationwide in scope, to ensure that visiting relief agencies are afforded access privileges consistently.

Type of Priority

Priority access can take any of several forms. In its simplest configuration, calls held due to system unavailability are placed in a queue. Users with priority access would go to the top of this queue ahead of all other non-priority callers. A more complex scheme would create a hierarchy of access, in which fire and rescue users might have a higher priority, for example, than traffic control personnel. Such priority assignments are discussed above in the Regulatory section. Finally, in extreme cases, a high priority user might cause a low- or no-priority call to be terminated in progress.

Priority to terrestrial and satellite communications systems may be assured in several ways. Channel priorities may be implemented by techniques ranging from access to the next available channel to preempting existing users. Preemption has practical and public relations difficulties. A critical EKG transmission could be preempted inadvertently by an operator for another emergency.

12.9.6.6 Spectrum relief

Public safety agencies are increasingly finding new roles for commercial services which did not previously exist, yet substantially lighten the load for dispatchers, by directing routine traffic to alternate, commercial spectrum. This is achieved by shifting computer inquiries from voice to direct data interface thereby relieving the voice channel loading.

The Alexandria, Virginia Police Department provides a good example of how moving to a commercial data service may relieve an overcrowded voice channel.

According to PSWAC/ISC 96-04-036 notes from a meeting at the Alexandria Police Department Headquarters, a cellular digital packet data system is under current evaluation as part of a pilot test. A CDPD network will be used to support laptop/notebook computers with wireless modems for data transfer. According to the report:

The Alexandria PD representative stated that the system initially will be used to request tag checks, wants and warrants, which are currently handled on a voice channel through the central dispatcher, who then accesses the data base in Richmond. The Alexandria PD currently operates on one dispatch channel and it routinely becomes overloaded during peak traffic periods. This has created delays of up to fifteen (15) minutes, during some peak periods, to get a routine license check called in to dispatch, and depending on the dispatchers' traffic load, the response back to the officer is significant. Consequently, in some cases the officers do not conduct a query

due to the time required to get on the channel. They feel the use of CDPD, will help to minimize both problems, first it is estimated that the voice traffic will be reduced by at least 30%, while reducing the response time of such data queries, and second, the officers will accomplish more queries, which they feel will increase the capability to recover stolen vehicles and apprehend offenders. The response time experienced during the test has been as little as two (2) to three (3) seconds from the time an officer inputs the data until the time he/she receives the response. Realizing as the system is loaded the response time will likely increase, the users are confident that the response time will remain significantly short.

If the initial pilot test is successful, the officers will eventually utilize the system to provide incident reports from the scene, which will relieve some of the officers' administrative burden, as well as possibly further reduce voice traffic by as much as another 15-30%

Groton, Connecticut Police Department uses CDPD with mobile data computers for messaging and to query the National Crime Information Center run by the FBI and motor vehicle bureaus throughout the country. Public safety officials can wirelessly exchange forms or messages from their vehicles or desktops within seconds. Previously, if an officer needed certain information, he/she had to call into the dispatch operation to get someone to pull the data and they relay it verbally. This was a slow process and discouraged people from asking for what they needed. (Ref. ISCWG9025)

The Philadelphia Police Department plans to install 70 laptop computers into Philadelphia Police vehicles to give officers access to reliable, timely information before they approach a vehicle, house or suspect, allowing them to accurately assess potentially dangerous situations. The software allows officers to connect to national, state, and federal data bases, police computer, the National Crime Information Computer (NCIC) and the Bureau of Motor Vehicles.

According to the software vendor, the software package saves precious time by only requiring police officers to make a single entry on their mobile data terminals versus what may now require a number of inquiries through the police dispatcher.

12.9.6.7 Commercial Security

The Philadelphia Police Department has plans to install 70 laptop computers into Philadelphia Police vehicles to give officers access to reliable, timely information before they approach a vehicle, house or suspect, allowing them to accurately assess potentially dangerous situations.

In addition to saving time, the mobile data terminals will increase the security of police department communications, because data is currently more difficult to monitor. Messages carried by CDPD are "encrypted" or scrambled with a "public" key to increase protection from unauthorized reception. The system is also capable of

end-to-end Type 3 (DES) encryption with the addition of encryption devices on all the mobile units.

12.10 Working Group #10 Report (Address Baseline Technology for Interoperability)

12.10.1 Report Scope

This report outlines the activities of Working Group #10 of the Interoperability Subcommittee (ISC), which was formed on February 29, 1996. Although the report addresses the comments and proposals introduced during the working group activities, all the details of the comments and/or recommendations are not reflected. However, all comments submitted are available for review.

12.10.2 Background

A proposal to adopt a baseline technology for interoperability was introduced in January, 1996 at the University of California Berkeley during the PSWAC Technology Subcommittee (TSC) meeting. Subsequently, during the same meeting, a proposal was introduced to identify the APCO Project 25 Common Air Interface (CAI) as the "air interface" to provide "unit-to-unit" interoperability. The Vice-chair of the TSC "tabled" both proposals for further consideration and there was little discussion at that time. After some deliberation, the PSWAC Steering Committee considered the subject and tasked the ISC to "address a baseline technology for interoperability", with the concurrence of the chairs of both the TSC and ISC.

The original proposals, previously introduced in January, were then introduced to the ISC members during the meeting in Orlando, Florida on February 29, 1996. The ISC Chair emphasized that the "tasking" was to "address a baseline technology for interoperability and consider a recommendation which may be that no recommendation be made". Recognizing that no conclusion would be reached during the meeting, the chair allowed extensive discussion concerning the proposals. However, during the discussions the subcommittee did agree to "address and consider" a Baseline Technology for Interoperability, with no further commitment at the time.

The ISC Chair requested that comments be submitted within two weeks with recommendations. The chair also formed Working Group #10 (WG10) to address and consider a *Baseline Technology for Interoperability*.

12.10.3 Task

The Chair of the ISC formed WG10 with instructions to consider and address a baseline technology for interoperability. The working group was tasked to consider the following:

- Should a baseline technology (for interoperability) be recommended?

- If so, what technology or methodology should be considered?

- Should the recommendation be mandatory?

12.10.4 Working Group Members

The ISC Chair solicited volunteers to participate in the working group and thirty-two (32) people, six (6) representing the manufacturing community and commercial service providers and twenty-six (26) from the user community. A chairperson was appointed (by the ISC Chair) from the list of volunteers.

12.10.5 Comments/Discussion

During the discussion that ensued during the Orlando meeting, it became somewhat clear that there was some confusion between what was meant by the word "technology", as opposed to the word "standard". The ISC Chair stated that it was outside the scope of the subcommittee to consider or recommend a "standard" and the discussion should focus on basic technology, such as wideband (25 kHz channel bandwidth) analog FM[19], narrowband (12.5 kHz or other bandwidth) analog, or narrowband digital.

In addition to the three recommendations introduced in Orlando, during the ISC meeting, there were eleven additional comments/recommendations provided, two were from manufacturing representatives, one from a commercial services provider and the remaining eight from the user community. The two responses from the manufacturers' representatives were in basic agreement that the baseline technology should be analog FM.

All respondents, representing the user community, agreed that analog FM technology be adopted as the baseline technology for interoperability, and after discussion, all agreed that the immediate technology should also be 25 kHz channel bandwidth, because that is all that exists in commonality today. However, the users expressed a desire that the baseline specify a narrowband (12.5 kHz channel bandwidth) analog FM technology as equipment migrates to narrowband operation in accordance with the NTIA mandate, for the federal users, and the FCC Re-farming Report and Order.

Most commenters agreed that the recommended baseline should be a mandatory requirement, but there was no clear choice on how the requirement should be enforced.

12.10.6 Recommendation

A conference call, for all members of Working Group #10, was conducted on April 4, 1996. The conference call was announced to all WG members, via facsimile, on March 29, 1996.

---

[19] One working group member pointed out that FM (frequency modulation) is a "defacto standard". While there is no "numbered" standard for FM, it is codified in FCC Rules and Regulation and NTIA requirements, as well as IEEE and TIA publications.

Thirteen, of the thirty-two members, participated in the conference call. The eleven written comments, which were previously distributed, were discussed and a number of recommendations were introduced.

The participating members of WG10 unanimously adopted the following recommendation to be submitted to the full subcommittee for consideration:

It is the recommendation of the Interoperability Subcommittee that the minimum "Baseline Technology for Interoperability", for unit-to-unit voice communication, be 16K0F3E (analog FM), unless Federal Communications Commission (FCC) and/or National Telecommunications and Information Administration (NTIA) regulations stipulate a different emission in a specific operational band. This mandatory requirement should be adopted as soon as possible by the FCC and NTIA. This recommendation is applicable public safety spectrum between 30 MHz and 869 MHz.

Effective January 1, 2005, the minimum "Baseline Technology for Interoperability", for unit-to-unit voice communication, should be mandated as 11K25F3E (analog FM) in public safety spectrum between 30 MHz and 512 MHz, unless FCC and/or NTIA regulations stipulate a different emission in a specific operational band.

The maximum allowable interoperability bandwidth in any new spectrum allocation should not be allowed to exceed the bandwidth established for operational communications within that new spectrum.

It should be noted that the above recommendation was modified during the full ISC meeting on April 12, 1996, in San Diego.

12.10.7 Dismissal of Working Group

Upon the revision and unanimous adoption of the recommendation by the working group, the ISC Chair thanked the members for their timely effort and dismissed Working Group #10 from further activity.

APPENDIX A
Interoperability Link Implementation Option Matrices

A-1 Interoperability Implementation Options

1.1 The following general abbreviations and structure are used in this Appendix:

1.1.1 *The "General Govt" category pertains to those important general governmental operations of local, state and federal agencies (general administration, hazardous materials management, mass transportation, public works, school bus safety, etc) which are eligible under the accepted definition of public safety, but which do not fall into one of the other established service categories.*

1.1.2 *Those function of general government, forestry conservation and highway maintenance which would make them eligible to use criminal justice, EMS or fire frequencies for their daily operations (eg: the fire suppression functions of state forestry agencies) also make these agencies eligible to use corresponding interoperability frequencies defined in this Appendix.*

1.1.3 Each use is designated by a number and a letter (1R, for example). The number represents the quantity of links required for this specific application. The letter is either "R" for repeatered links, or "S" for simplex links. Note that each "R" link requires 2 separate talk paths (eg: a "4R" designation requires 8 talk paths).

1.1.4 With the exception of the 806-824 MHz band which has no service-dependent designations for any frequencies, the designation of a link under a specific category generally means that the link is being recommended to be provided from frequencies assigned to that service.

1.1.5 Footnotes are listed for each use which show where it is recommended that currently assigned frequencies be used to meet the requirement. If the requirement can be fully met using currently designated interoperability frequencies , it is marked with an asterisk (*), if the requirement can be partially met, it is marked with a plus (+).

1.1.6 An "X" in any column indicates that this user category has full access to this link, unless a specific footnote states otherwise.

1.1.7 Channel Numbers shown in footnotes represent FCC-designated channel numbers; reference Appendix B.