

Communication Issues for Emergency
Communications Beyond E911

Report #1 - Properties and network architectures that
communications between PSAPs and emergency services
personnel must meet in the near future

1	Results in Brief	3
1.1	Executive Summary -- The Emergency Communications Internetwork.....	3
1.2	Future Reports	8
2	Introduction	9
2.1	Structure of NRIC VII.....	9
2.2	Focus Group 1D Team Members.....	9
3	Objective, Scope, and Methodology	10
3.1	Objective.....	10
3.2	Scope	10
3.3	Methodology.....	11
4	Background	11
4.1	The Changing Face of Emergency Communications.....	11
4.2	Users.....	12
4.3	Geography.....	13
4.4	Purpose.....	13
4.5	System Reliability and Design	13
5	Emergency Communications Future Needs	14
5.1	Key Characteristics of Emergency Communications Systems of the Future ..	14
5.2	Current and Future Data Sources.....	23
5.3	Redundancy and Reliability	33
6	Major Considerations and Recommended Actions	36
6.1	A Note on Transport v. Data v. Applications, and Tools v. Policies and Protocols	38
6.2	The Immediate Tasks.....	40
7	Outline of Recommendations.....	43
8	Appendix A - Samples of Data Types	49
8.1	Real time data from the public.....	49
8.2	Real time data from private sector providers	50
8.3	Real time data from other response agencies	50
8.4	Integrating data from multiple sources and forwarding it to agencies	50
8.5	Real time data between agencies and their staff in the field	51
8.6	Non-real time data from stored data bases	51
8.7	Interactive data.....	51

1 Results in Brief

1.1 Executive Summary -- The Emergency Communications¹ Internetwork

A critical weakness of the current emergency communications system is that agencies are isolated from each other. The only ubiquitous interoperability is via wireline telephones. That does not help emergency responders in the field, and it does not allow the sharing of data. Our emergency responders are being asked to do one of the most important jobs in our society, with communications and information technology that most businesses have moved beyond.

We are sending emergency responders into harm's way without information which they could have, and without the tools to stay in touch with their colleagues; we are asking commanders in offices and in the field to operate without the most modern tools, and the information those tools could provide. With the right systems and tools, we could have faster, and more informed, emergency responses.

The emergency systems we recommend are entirely consistent with, and should be the central nervous system of, the National Incident Management System (NIMS) and a modern Incident Command System (ICS). The primary method for Homeland Security agencies to receive appropriate data is to have an effective day-to-day emergency communications system -- that can then also be used in times of national emergency. The wrong method is to create "homeland security" networks or applications (or usually any other purpose-built system) in isolation.

We see the future emergency communications system as an "internetwork"² -- a series of secure local, regional and national wireline and wireless networks providing modern, integrated information capabilities to support local, regional and national needs, or a system of systems.³ The following Diagram 1 is an illustration from one

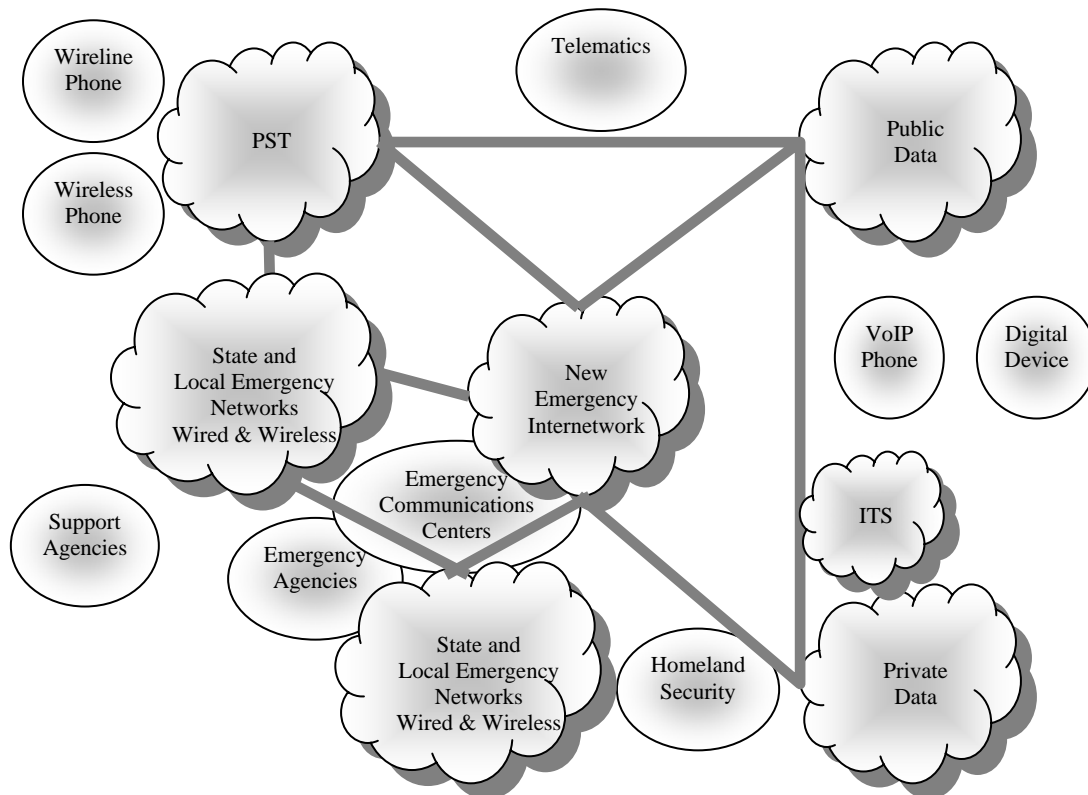
¹ We use the term "emergency communications" deliberately because it encompasses a broader scope of parties and organizations than the more traditional term "public safety communications." This paper, and we believe proper policy, recommends a seamless system connecting the public to emergency agencies, and those agencies to each other. The definition of "agencies" is similarly broad, encompassing any public, private or non-governmental organization which has a role to play in preparing for or responding to an emergency.

² We use this unfamiliar term to make two points: (a) our strong belief that the model of the Internet should be copied for emergency communications in the future (except for its failures until recently to focus proper attention on security), and (b) that we do not favor building a new "national emergency network". There are already many networks, and there need to be many more built at the state and local level. Our focus is on how to connect them into a seamless whole, rather than replace them.

³ "System of Systems." Public safety communications devices are associated with systems and networks that range in size from small to large. Whether large or small, the systems and the networks they use work with each other to pass information and communications back and forth seamlessly. In some cases new networks must be deployed by agencies, localities, regions, states, tribes or federal agencies. In other cases, we need to connect tools, systems, and networks that are already deployed. Our overall goal is that all systems together become a system of systems.

perspective of this “internetwork.” It seeks to show the various categories of participants and systems that will be connected from a national perspective. The two clouds of “state and local networks” merely hint at the multiplicity of state and local networks of wireline and wireless that will connect agencies and emergency responders in various ways. These are more fully displayed in Diagram 2.

Future Internetwork Architecture



Created October 25, 2004

Draft 1

Diagram 1: Future Internetwork Architecture

To achieve this vision, we strongly recommend that policy makers and others regard emergency agencies, both public and private, as an overall “enterprise,” rather than a collection of separate entities -- the multiplicity of unconnected and isolated islands we have today. An enterprise perspective will give planning and policy making coherence and comprehensiveness that have been previously lacking. However, unlike corporate information technology enterprise solutions, this enterprise will have neither a single owner, nor will it have a single physical network. The emergency internetwork will

have the same multiplicity of owners that exist in emergency response systems today – tens of thousands of agencies.⁴

Many of these have now developed interoperable wireless networks for their communities; others are devoting enormous efforts to achieve that critical goal. Radio interoperability has been a long-standing goal of leading public safety organizations, to which the federal government has recently committed significant attention through the Department of Homeland Security SAFECOM Program and grant funding. A much smaller number of communities are pursuing data interoperability between their emergency agencies, much less with the public in general.

This progress means that the number of “nodes” on an enterprise network may have been reduced, but the technical problems of connecting them through this internetwork remain the same. In addition, we have to devote major attention in the near term to develop the cooperative institutions to provide the policies to govern this new interconnected system. .

We believe the future emergency internetwork will be a network of networks, a series of separate physical and virtual networks interconnected seamlessly to help emergency agencies and their staff:

- Respond appropriately to local emergency situations
- Respond appropriately to larger scale situations requiring the aid of neighboring agencies, often referred to as “mutual aid”
- Respond appropriately to very large-scale incidents requiring assistance from a large number and variety of responders from many different areas including national agencies

This emergency internetwork will link the public to emergency agencies, and link them to each other. It will enable both faster and more informed response. It will empower emergency agencies to have far more control over information flow and use than they have today. It will save them time and money in daily use.

Diagram 2 provides a more detailed view of the internetwork we envision. It shows how wireline and wireless networks of different levels of government and agencies can interconnect with each other and the public.

⁴ We think it is fair to assume that there are about 120,000 organizations which would be connected to the internetwork, not counting schools (140,000+), private employers or others which should be part of the broader two way public emergency messaging capability of the internetwork.

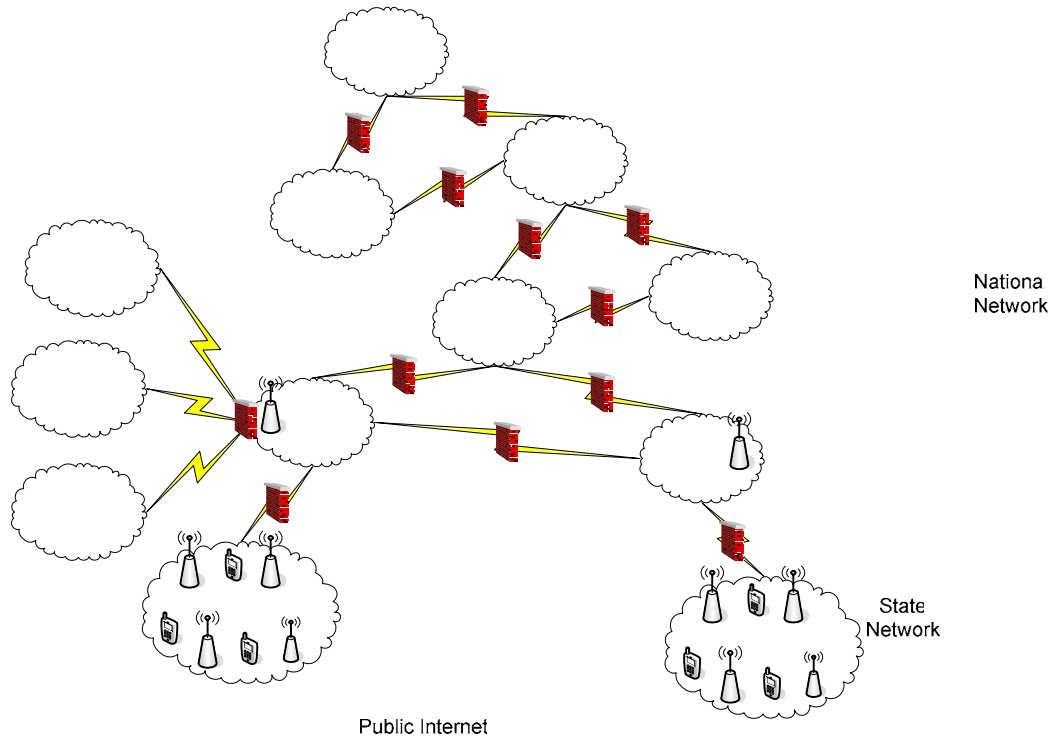


Diagram 2: Interrelationship of Networks in the Internetwork

This paper discusses our vision of emergency communications. That vision is summarized as follows, and partially illustrated in Diagrams 1 and 2, and Diagram 3 below:

PSTN

- (1) A single, interconnected Internet Protocol network should be used for all emergency communications, connecting a wide variety of agency-run and public networks, both wireline and wireless. We call this an "Internetwork" to emphasize that we do not believe a new physical network is needed. We recommend a system of systems approach.

Non-Traditional
 First Responder
 Networks

- (2) All layers of emergency communications should rely on international, open standards, preferably borrowed from non-emergency communications needs where possible. Standards themselves should be set by internationally or nationally (if appropriate) recognized standards organizations such as IEEE, IETF, OASIS, ITU and TIA.

Jurisdiction Communications
 Network

- (3) Access to network and information resources, i.e. security, should be governed by cryptograph-ensured access control, not separate physical networks. Access control also implies both authentication and authorization for system use. Authentication is defined by both user and source identities and authorization confers system rights.

- (4) Data and networks should be organized in a distributed, not a hierarchical, architecture, embracing a multiplicity of communications pathways and methods. We should have common coordination and facilitation functions for cryptographic certification, authorization policies, message routing (i.e. directory), and resource discovery. This includes data sharing and connecting disparate elements in this interoperable architecture. Diagram 3 demonstrates several methods of data sharing, and these common facilitation services, specifically:
 - a. Direct agency to agency communication with no intermediation
 - b.
 - c. Use of a service where agencies post data to a server, and/or can poll from one when they wish. Agencies can access common "facilitation services" directly
 - d. Agencies can use intermediary providers which use the "facilitation services."
- (5) XML-based data elements for interchange of common emergency-related information should be defined. Where these do not exist, they should be developed by open processes of all emergency agencies, not by specific sectors.
- (6) All communication should be protected to ensure privacy and integrity of the communications.
- (7) The same network infrastructure, protocols and applications should be used during all emergency operations. Shared networks should be encouraged to reduce costs.
- (8) There is a small set of core application-layer protocols that should be specified, namely for event notification, session setup and resource discovery.
- (9) We recommend immediate action on the "The Immediate Tasks" described in Section 6

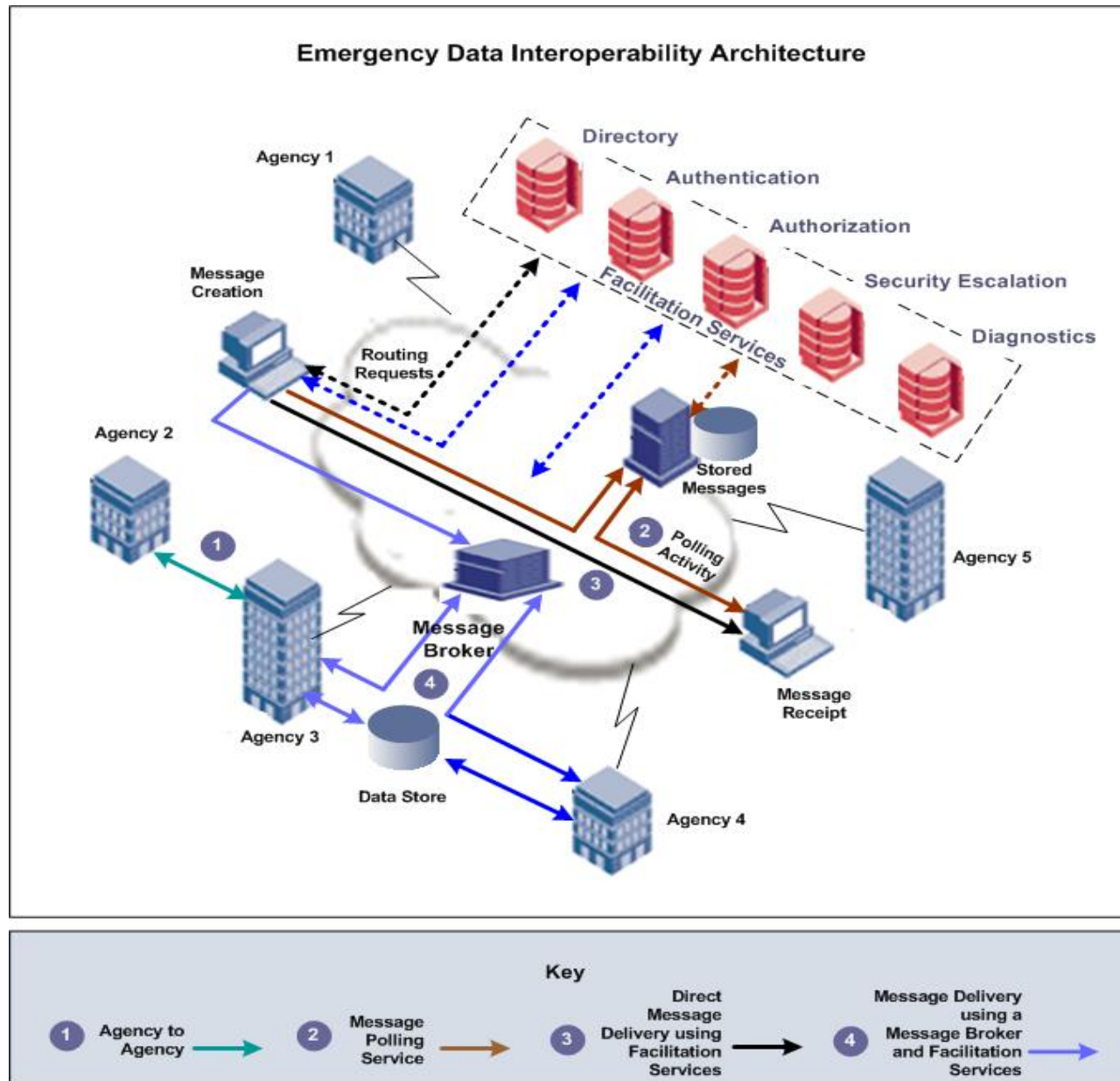


Diagram 3: Emergency Data Interoperability Architecture

1.2 Future Reports

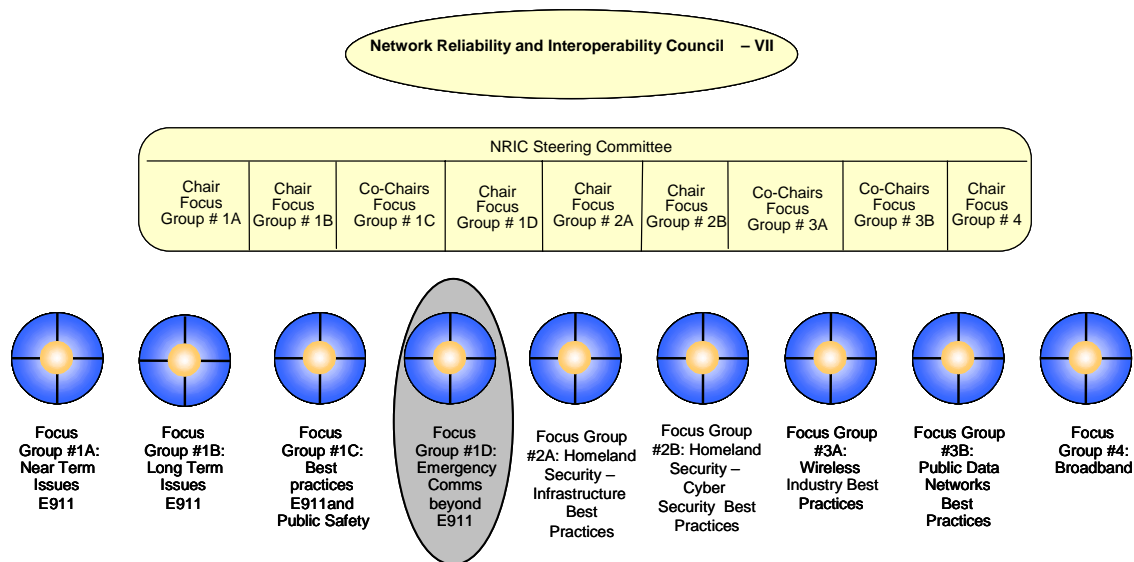
Contents of future reports from Focus Group 1D will include the transition issues for the recommended target architectures, and a proposed resolution of these transition issues along with a time frame for their implementation.

2 Introduction

This report documents the efforts undertaken by the Network Reliability and Interoperability Council (NRIC) VII Focus Group 1D with respect to the long term network requirements for transmitting emergency services information that is beyond the scope of E911 networks.

2.1 Structure of NRIC VII

The structure of the Network Reliability and Interoperability Council is as follows:



2.2 Focus Group 1D Team Members

Today, Focus Group 1A consists of 27 members, as listed below.

Focus Group 1D Members

Name	Company
RoxAnn Brown - Chair	Metro Nashville Emergency Communications Center
Dennis Pappas	Qwest
Roger Hixson	NENA
David Aylward	ComCARE Alliance
Sukumar Dwarkanath	ComCARE Alliance
Kamil Grajski	Qualcomm

Mario DeRango	Motorola
Rich Galitz	Motorola
Dale Morgenstern	AT&T
Wie-Sian Oei	Intelsat
Charles Werner	Charlottesville (VA) Fire Dept.
Brian Rosen	Marconi
Henning Schulzrinne	Columbia University
Darryl Foster	Cox Communications
Amarjit Deol	Nortel
Robert Schafer	MCI
Tom Steel	IACP
Stuart Goldman	Lucent
Doug Rollender	Lucent
Stu Miller	Intrado
Gerald Callejo	Intrado
Jeng Mao	NTIA
Michael J. Mangini	Plant Equipment
Marilyn B. Ward	Orange County Public Safety
Percy Kimbrough	SBC
Marty Feuerstein	Polaris
Bob Dressler	Polaris

3 Objective, Scope, and Methodology

3.1 Objective

The NRIC VII Council has been charged with defining the long term network requirements for transmitting emergency services information to emergency services personnel that is beyond the scope of E911 networks. This includes the identification of architectures that will be able to transmit the needed information about emergency events to all persons and agencies which need it, and to aid in coordinating emergency services activities.

3.2 Scope

This document addresses the first two deliverables outlined in the NRIC VII charter for Focus Group 1D:

- 1) The Council shall present a report describing the properties that network architectures for communications between PSAPs and emergency services personnel must meet by the year 2010. These recommendations shall include the access requirements and service needs for emergency communications in the year 2010.

- 2) The Council shall present a report that recommends the network architectures for communications between PSAPs and emergency service personnel that can support the transmission of voice, pictures (e.g., from a cellular phone), data, location information, paging information, hazardous material messages, etc. The report shall describe whether and how IP technology should be used.

In this report, Focus Group 1D makes specific recommendations on the following four issues outlined in the NRIC VII Charter:

- Whether IP architectures should be used for communications between PSAPs and Emergency Communications systems and personnel and, if so, how it may be used.
- How methods for accessing Emergency Services Personnel by PSAPs should be modernized.
- Architectures that will allow PSAPs (or other network elements) to send text, pictures and other types of data, such as automatic crash information, to Emergency Services Personnel.
- The most appropriate role of 911/E911 in major disasters and for terrorist attacks.

3.3 Methodology

The Focus Group members participated in a number of conference calls and face-to-face meetings to develop the recommendations in this report. Additionally, the report was cross-referenced with those recommendations previously made by Focus Group 1B to ensure consistency across Focus Groups.

4 Background

4.1 The Changing Face of Emergency Communications

Traditional emergency communications have been voice-based: telephone and radio. Until recently, data was entering information into a computer after an incident. Real time data sharing to support incident response has become more common in recent years, but almost invariably is limited and confined to the members of a profession (e.g. police and fire mobile data units communicating with their headquarters, and then to foreign data bases for limited purposes, e.g. NCIC). An FCC-sponsored study by Dale Hatfield pointed out the inability of the current 9-1-1 technologies to accept external

and dynamic data.⁵ A recent article by two leading 9-1-1 experts details this critique, and argues for adopting open XML-based architectures such as those recommended in this paper⁶.

Even discussions of interoperability have been generally confined to radio use in response to a localized incident until recently with the advent of the SAFECOM Statement of Requirements and the standardization of the 4.9 GHz band. While those issues are critical and must be resolved, information sharing and interoperability must be addressed in their full scope.

All that is changing based on new technology, demands of homeland security, and new commercial products which produce data for emergency response (e.g. E9-1-1, telematics). Emergency response increasingly requires seamless voice interoperability across disparate mobile systems and the ability to exchange relevant data: across a city, across professions, and across a region or the country. While an incident may be purely local, event data or knowledge necessary to respond intelligently may well reside elsewhere. Nowhere is this truer than in a major terrorism incident or other mass disaster where the numbers of responders, victims and issues are most likely to be very large. It is simply not possible to handle events requiring multi-agency responses efficiently or accurately with voice communications alone, or with only data communications from a command center to its staff at the scene. This is equally true of Amber alerts.

A wide variety of data sources are developing which need to be handled by emergency response officials. Many of these can be found in the Project SAFECOM requirements paper recently issued by the Department of Homeland Security.⁷ Others are described in the attached Appendix A.

4.2 Users

The emergency response internetwork needs to accommodate a wide range of government agencies, non-profits, private sector businesses, and the public. For economy in word use, we use the term “emergency agency”, but we intend it to have a very broad meaning. The users of the network will be any and all organizations that improve the safety of the public by being able to exchange information in emergencies.⁸

⁵ See Hatfield Study of E9-1-1 for FCC, 2002.

⁶ See Meer and Nelson, Submission to ATIS, June, 2004

⁷ See also, Bass, Potter, McGinnis and Miyahira, “Surveying Emerging Trends in Emergency-related Information Delivery for the EMS Profession”, Topics in Emergency Medicine, Vol. 26, No. 2, April/June 2004, pp. 93-102.

⁸ The SAFECOM Statement of Requirements semantically drew a distinction between “public safety providers” (agencies in a more traditional safety sense) and “public service providers” (support organizations).

Network access will vary among these groups depending on circumstances, but they should be part of the same internetwork.

4.3 Geography

We believe the primary focus should be on the United States. Coordination with Canada and Mexico is desirable. Yet, most of the communications technology that will be employed to make this vision a reality is international in scope, in standards and in applicability. We believe that we must work closely with international standards organizations to define many of the actual communications standards to be deployed. Internationalizing the effort will have other positive effects: for example the market will be larger, making costs for acquiring the required technology lower.

4.4 Purpose

Our goal is to enable the real time sharing of information across the processes and functions of fixed enterprise and mobile environments to make emergency response more informed, safer for the participants, and more effective in outcomes. A fundamental principle for the future is to empower emergency staff. This future needs to be user, not vendor, driven. Information needs to be provided where it is needed, when it is needed, to the people and agencies that need it. That tends to drive intelligence to the edge, minimize approval and “vetting” processes (or push them to point of creation, prior to need), and to avoid “gatekeeper” functions.

Our goal is to empower the appropriate chain of command with new tools and capabilities. This means that the system needs to be highly flexible, with mechanisms which allow very different information flows depending on the need of the moment.

One important aspect of information sharing in this field is that for the first time we will be creating end-to-end incident records which will provide a serious base for research, relatively inexpensively, because this data collection will be a byproduct of daily use.

4.5 System Reliability and Design

The system must be extremely reliable. Reliability has several components. Two primary methods of achieving that will be (1) the redundant nature of the internetwork⁹, and (2) multiple access points to it from other agencies. Further, the data should be distributed (not one large database, but multiple smaller ones), replicated

⁹ See footnote 6.

(not only redundant copies for reliability, but cached close to point of need for accessibility when reachability of the network is compromised), standardized (primarily XML formatted with standardized schemas), and secure (authenticated access, role based authorization, and privacy and integrity where needed).

In addition, packet switching is inherently more efficient than today's circuit switched networks. It is more likely to allow completed communications in a high usage situation (although the packets may be slowed down).

The Internet is an excellent model for us, both in positive and negative terms. Except for the lack of attention which was paid to security until relatively recently, we believe it is the model which should be followed.

- **Separate transport from applications**

Public safety has had a tendency to intertwine transport protocols and methods with the data they are carrying. Thus, we have a PSAP network for location data, and another (law enforcement) one for crime information. One of the reasons for the great success of the Internet was the complete separation of the two, and agreement on one transport protocol: IP. We propose to use this model as well as many of the Internet protocols.

- **Separate applications from types of data**

In a similar way, we believe we can make the most progress, most efficiently, if we separate applications from different types of emergency data, or at least emergency messages. In other words, it should not matter to a 9-1-1 CAD system that it is receiving a telematics message from OnStar, a bio-terrorism alert from CDC, or data about a 9-1-1 call from a wireless company. The same system should be used.

- **Common directories**

A limited number of private and/or non-profit entities provide a quasi-governmental function in providing addressing for the Internet. That model should be followed in the future as well.

5 Emergency Communications Future Needs

5.1 Key Characteristics of Emergency Communications Systems of the Future

5.1.1 Handles wide range of data

In Appendix A we describe many of the types of data that will become available to response agencies. There is also an extensive list in the SAFECOM Statement of Requirements. The internetwork must be able to handle voice, data and video, and large amounts of all those. The issue will not be the content of the data, but rather the amount of it, the required bandwidth (e.g. for video), and acceptable quality of service for these applications.

5.1.2 Easy to use and intuitive

The best technology is useless without users, and training budgets are stretched. Systems need to be developed with simple user interfaces and other attributes which promote ease of use.

5.1.3 Access rules

Agencies should have the right to control access to the voices and data on their systems. The internetwork needs to allow owners to decide whether or not to publish their data and to permit access to their fixed and mobile data environments. If an agency chooses to make data available to others it must be able to “tag” its data, and have that restriction enforced throughout the network. This is a critical feature in getting “buy-in” to interoperability.

Data is more accurate when the actual creator of the data is responsible for publishing it. When many levels of administrative management stand between the originator of the data and the publisher of the data, it gets out of date, inaccurate and incomplete. The network should make it easy to publish data. Data should be published in small parts that are aggregated by the network, rather than coalesced into very large data warehouses.

5.1.4 User controls the data they pull from the network

Agencies should be able to decide what data they want, for what area, how they want it delivered and how they wish to access it. They should be offered the ability to have data pushed to them, or to pull it, and to designate the delivery points.

5.1.5 Standards-based

Standards serve a variety of positive purposes. Economically, they improve quality and reduce acquisition costs by creating a large national and international market. Improved R&D increases customer choice of components. The current system is characterized by a large number of proprietary systems. Even where there have been

efforts made to standardize data, interfaces and access protocols these have generally been confined to professional areas, e.g. EMS, criminal justice, transportation, 9-1-1. This is a serious problem when the emerging demand for access to networks and systems is between professions, not just within one. It is only very recently that there have been conversations between these entities, but there is no aggregate emergency standards coordination effort, let alone one to produce common standards for all emergency response agencies.¹⁰

Wide use of commercial standards lets emergency services networks be built from Commercial Off-The-Shelf (COTS) hardware and software. COTS network elements offer lower costs, more choices, and ready access to skilled network and software engineers.

Government leaders should first look to existing commercial standards and commercial standards processes, and then existing ones in specific sectors of emergency response, before inventing special ones for public safety.

5.1.6 Multi-use, multi-user

A key aspect of the internetwork, and for most of the networks which underlie it, is that it will be for all emergency uses, and for all emergency users. Indeed, in many instances, with appropriate protections, it should be shared with non-emergency users. This will lower costs and increase interoperability. There may be specialized applications for handling data across enterprise and mobile systems for particular professions or incident types, but the underlying network and standards should be shared.

The military have a saying which applies here: train the way you fight, and fight the way you train. Systems which are accessed by responders only during “the big ones” will be far less useful than those on which they are fully trained because of daily use.

5.1.7 Session negotiation: tell me what I can do: video, voice

Endpoints will come in many sizes, shapes and capabilities. The capabilities of this equipment will vary. Yet all need to be able to communicate. The capabilities for each session (call) should be negotiated among the endpoints at session initiation. Standards should specify minimum capabilities to assure that everyone can communicate at a minimal level, with additional capability available when all participants in a session have higher levels of capability.

¹⁰ As noted in a number of other places in this paper, we compliment and encourage emergency standards efforts in various areas. For example, we strongly support the long standing effort by police, fire and other agencies and their vendors to produce and implement a common air interface for radios, the P25 standard. Other emergency sectors (e.g. Justice, transportation, EMS) have undertaken major efforts to develop common data sets.

5.1.8 Unified registration system

There must be a registry that allows agencies to inform others about the availability of communications systems, access and interface protocols, resources, events and data they may have available. Agencies need to be able to register in a secure location-based utility (or system of utilities) for receiving incident data, expressing what incident information they want, for what geographical area, and how and where they want it sent to them. There must be a trusted process to authorize entries and use of such registries. There need to be other, more open registration systems for individuals and businesses, e.g. for public warnings.

With so much data available, knowing what is available and how to get it becomes problematic. There must be registries for data made available where sources of data can advertise availability, nature, extent and applicability of the data as well as the access mechanisms deployed to it. These registries must be available to all agencies, as it is impossible to predict who will need the data when emergencies occur. Web services is a very useful technology in this regard.

5.1.9 Control authorizations; flexible rule sets

The internetwork must have a common facility to control authorizations, to have them provided in a known, trusted system. Authorizations for both agencies and individuals should primarily be role based. We need to allow incident commanders and dispatchers to adjust authorizations to fit on-the-ground conditions. While it might be useful to develop a classification system for defining voice and fixed data access, there are limits to the complexity these systems can manage. Cooperating applications can implement reasonably simple rule sets that can be published, but having more comprehensive systems with system-guaranteed authorization enforcement is currently an unsolved problem.

5.1.10 Universal authentication

Authentication is one of the cornerstones of the security mechanisms foreseen for the internetwork. There must be a trusted way to credential agencies and individuals, provide them with appropriate authorizations, and allow them access to and use of the network. Mutual aid, regional disaster and national disaster response must not require security to be compromised, which implies that the authentication system should be comprehensive and capable of extending access to out-of-area agencies and responders quickly and securely. This implies some national credentialing hierarchy.

There is a critical distinction between authenticating based on device or by agency/person. The traditional way with radios is to do it by device. This raises

security problems (mere possession of a device does not mean the person should be using it). The better solution is to authenticate by person or agency. However, cultural and user convenience issues of single sign-on need to be addressed technically.

These latter three pieces – Unified Registrations, Control Authorizations, and Universal Authentication – are perhaps the most difficult parts of the internetwork to be implemented and maintained. Beyond technology, they require major policy processes (at every level of government), and involvement of every emergency agency in the country. Today we lack the institutions to accomplish this. For fully effective use, we will have to harmonize state laws that address information sharing and privacy, and we will need to provide the resources to implement these systems. In order to minimize this resource barrier to deployment, these need to be done as shared utilities. Many emergency response agencies do not have the resources to field such systems on their own.

5.1.11 Congestion control (packet priority)

Data and media streams will compete within limited bandwidth available on the internetwork. As with many things in major emergencies, there may never be enough bandwidth. However, exploration of solutions for congestion control and prioritization may determine that more bandwidth is cheaper than applying priority systems. This is particularly true for wireline communications.

The internetwork will need a common set of agreements on congestion control¹¹. Will voice always be first? We do not believe such a bald assertion will be valid.¹² In some circumstances various grades of data may be the more important priority. While mission-critical voice will always need to have a very high priority, administrative and non-emergency voice communications may have a lower priority than some data transmissions (incident dispatch, for example), consistent with network capabilities. Similarly, does the individual or agency dictate priority, or should it be the type of message or the content of the communication? The agreements will need to address questions of who will determine these priorities, how to achieve adoption of the rules and what mechanisms are needed to modify or update the rules.

Media handling endpoints should have capability to negotiate bandwidth – trading off media quality for bandwidth. The network needs mechanisms to notify endpoints of current network conditions, and local policy so that such negotiation will result in maximum effectiveness of a scarce resource.

¹¹ This is one more example of a function that will need to be performed by one or more of the new cooperative institutions and partnerships that will be required by this interconnected system of the future.

¹² For example, consider silent data dispatch. Further, radios are sometimes on the fringe of coverage areas and may be able to reliably transmit and receive data when voice transmissions are not possible.

Signaling priority mechanisms, in conjunction with Call Admittance Control, could allow preference to the establishment of an emergency response call, while other calls are being rejected because of overload. Strong Call Admittance Control may sufficiently address the quality of service issues in many networks.

While many of the networks in the emergency services internetwork will be built specifically for government use, we expect that public networks will be used both as an extension of government owned networks and as links within a government owned network (such as in virtual private networks). And, as noted elsewhere, we strongly encourage the use of commercial off-the-shelf devices and network elements in emergency networks. It is therefore necessary to understand the rules used by such network elements as they may not be consistent with all of the priority mechanisms in a purpose-built government network. For example, the mechanisms being developed for the Emergency Telecommunications Service (ETS), which are likely to be deployed in many public networks could be “re-used” in whole or in part for addressing some priority issues.

5.1.12 Multiple levels of priority setting

There must be a system of assigning multiple levels of priority to IP communications both based on message content and the identity of the sender.¹³ All elements of the internetwork will have to honor the priority of the data. Priority must be provided for both the signaling and the media streams.

For the signaling, methods are being standardized that provide priority for session establishment similar to existing mechanisms such as the Multi Level Priority and Pre-emption (MLPP) system used by many DoD systems.

In addition to the session establishment priority, the packet streams themselves, including media stream packets, need priority mechanisms. Existing IP standards such as DiffServ might be used to implement this priority mechanism, but standards will need to be created to specify how to classify the data, precisely how to mark it, and precisely how the different levels should be treated by the network.

Unlike the systems available for emergency communications today, IP networks allow flexibility in establishing priorities of communication at the network layer, and in regulating how much traffic is allowed into the network under certain circumstances. By using the IP “DiffServ” mechanism, packets representing various traffic classes (voice, video, routing data, routine data,) may be “marked” with a “DiffServ Code Point”. Each router can then be instructed how to treat each class of traffic. Since the routers in a network are under the management control of the owners of that network,

¹³ See SIP resource priority provisions.

they can make their own decisions on how to treat the classes. So, for example, one county may make responder voice communications the absolute top priority, while another county might have critical data (for example, an “evacuate immediately” message) have higher priority than responder voice. A packet marked with the responder voice code point would have priority on one county’s network, but if it was routed to the other county due to a mutual aid situation, it would have the priority of that county on its network. It is even possible to have different priorities on, say, a limited bandwidth wireless network than on a high bandwidth wired network for the same code point. To make this work, we must have national agreement on the markings, but then we can support local decisions on exactly how each class of packets will be treated on the local network. Of course, most routine data traffic will be unmarked, or treated as “best effort” traffic which is the norm on most IP networks.

In addition to the traffic marking and router treatment of such packets, we can specify and deploy “Call Admission Control” mechanisms for packets representing an identifiable “session”, such as a voice conversation between a specific set of people. The users can be given permissions for, and can automatically or manually apply a priority to a session. We can implement preemption of lower priority sessions when higher priority sessions are initiated. Using such mechanisms, we can be reasonably assured that the network will not become overloaded with high priority traffic. We will only “admit” enough such traffic as the network can handle. To be sure, it is often difficult to assess precisely how much traffic can be supported, but reasonable heuristics can be used to allow reasonable results (high utilization with low collision rates). We also caution that most data traffic on an IP network is not constrained to be part of a session for which such admission controls are possible. It is the media intensive (voice, video, text messaging) applications that have a notion of session management.

Preemption of higher priority traffic over lower priority traffic should be implemented in all networks. Authentication and authorization must limit preemption capability. “Barge-in” facilities for all real time media streams should also be uniformly implemented. Voice preemption may not be legal in some circumstances such as wireless priority service.

These features are probably most important in local wireless emergency networks. Given the low price of bandwidth in wired networks, it may be cheaper to expand capacity than try to develop complex prioritization schemes that run throughout the internetwork.

Further, it is understood that the above discussion is applicable to the network layer (using the OSI model) of the network, and not the physical or medium access control layer of the network. Priority treatment of traffic may also be accomplished at the physical layer. Different physical layers may have different mechanisms for providing priority, and they may not be as flexible as the IP mechanisms. Networks must be

engineered to have priority mechanisms appropriate to the traffic, and as much as possible, be mapped to the overall local IP network priorities. Public safety will require some method to address priority at these lower layers in order to assure that mission critical communications do not compete for the medium in the same way non-mission critical communications will. An officer saying “Don’t shoot” should not have to compete for the medium with an officer who is downloading the day’s crime report.

5.1.13 Security

There are two fundamentally different approaches to security on large communications networks that have evolved. One is known somewhat colloquially as a “walled garden”. In this approach a network is physically restricted to only connecting to its members, with no interconnections to other networks. Communications within such a network are assumed to be safe. Inside the wall, the network is trusted, and there are no holes in the walls. Another approach is to assume that the network itself is open to everyone, and to use cryptographic mechanisms to assure that communications that must be kept secure are ubiquitously authenticated, integrity protected and private, where required.

Walled gardens are often employed in the most secure networks where the effort to control all the access points is feasible. Walled networks have the highest possible security. In the significant networks with a large number of different kinds of users that are the kinds of networks emergency communications must have, it is very difficult, if not impossible to maintain a walled garden. The networks are too large, and too diverse, and we need interconnections between government networks and public networks in order to do the kinds of things we envision in this report. Indeed, the largest problem in maintaining walled gardens is to make sure no one deliberately, or inadvertently, creates a hole in the wall.

In the past, it has seemed easier to physically restrict users on special purpose public safety communications networks, i.e. create a walled garden. We believe it is no longer appropriate to do so, and thus we advocate that we do not continue to create “walled garden” networks, but rather that we apply uniform, cryptographically based authentication, authorization, integrity protection and privacy controls to all networks that emergency communications must happen over. We specifically believe that we should not “trust the network”. Rather we think that every communication should be considered to be transiting insecure networks, and thus needing cryptographically based security. We believe that public safety agencies should take reasonable precautions to assure that their networks cannot be used by unauthorized persons, but we argue that we should not assume that such precautions will be enough.

We should focus on deploying appropriate security mechanisms on top of the basic packet transport infrastructure to provide the security we need. Because we advocate a

mix of public and private IP transport networks, we will need the security discussed here to run at the session layer. We advocate that security be uniform. It should always be enabled, on every transport, for every communication.

The security we recommend includes:

1. Authentication, as discussed above, which should identify users and not devices, be public key based, and rely on a national PKI to allow credentials to be accepted from one agency to another as the need arises.
2. Integrity protection. In all cases, data should be integrity protected against modification ("Man in the Middle" attacks).
3. Privacy. In most cases, privacy (encryption) of data will be required.

If the protocol used for communication is TCP, we recommend TLS be used as the standard protection suite. Where TLS cannot be deployed, and the protocol does not specify an appropriate security mechanism, IPSEC tunnels should be established between parties so secure communications can be established. Appropriate algorithm choices would be RSA-1024/SHA-1/AES or the current FIPS equivalent. We recognize that these choices are only appropriate as this document was written, and will need to evolve over time as compute power, algorithm development and needs evolve. We further recognize that these recommendations present a significant challenge to vendors and systems designers to deliver this level of security in the variety of end devices that will be common, especially those with limited computing power and battery life.

Interconnection between public safety networks and public networks gives us much additional capability but raises some security concerns, especially when it is also necessary to connect public safety to highly secure federal networks. Where these networks need to interconnect to federal or other networks that are walled gardens, we must deploy carefully managed applications gateways at the edge of the walled garden networks that can allow secure communications of permitted data from such networks across our networks even when our networks are also interconnected with public networks.

5.1.14 Flexible addressing

All parties and systems associated with the internetwork should assume that all devices will need to be available on the public Internet, even though most will not be. When disasters strike, assumptions on infrastructure tend to fall apart. Flexibility is needed to respond. Systems needing well known addresses should rely on the Domain Name

System (DNS)¹⁴; dynamic DNS¹⁵ may be appropriate for many systems rather than on static address assignments. We advocate that public safety not deploy Network Address Translation devices (NATs),¹⁶ especially when IPv6 is used. On the other hand, systems are advised to assume NATs exist and deal with the discontinuities they introduce.

5.1.15 Diagnostics and solutions

The internetwork will be composed of multiple fixed and mobile systems tied together, very much like the current telephone network and internet. Like those, we will require the ability to diagnose and resolve a problem end-to-end. Each network will need to have its own network management structure, but there need to be some common standards. This means that a series of common elements will have to be developed and agreed to by the cooperative institutions set up to manage the internetwork. These will include issues such as alarming and outage reporting.

This process has been successfully undertaken in the telephone industry for 20 years since the breakup of AT&T ended its effective single company dominance of such issues. We should learn from those experiences.

On the other hand, we explicitly do not advocate a single over-arching management system. We believe such a system would be vulnerable to attack. Having more local management systems with some common characteristics is preferable. Just as with the proposed security solutions, this type of management structure implies adequate resources to manage it, and shared tools wherever possible to minimize the overall system costs which must be borne by any single agency.

5.2 Current and Future Data Sources

5.2.1 Overall

Additional information and transport media will make emergency response agencies better prepared to provide and coordinate resources in answering calls from the public.

¹⁴ DNS is the component of IP networks that lets users and programs refer to devices and services by a name, like "fcc.gov" rather than an IP address. The DNS translates names to addresses.

¹⁵ Dynamic DNS is a relatively new mechanism that allows the DNS to map a well known name to a device who's address changes from time to time, such as when it is assigned by DHCP; with DHCP its possible that a device gets a new IP address every time it "boots". Dynamic DNS allows the mapping of name to address to be changed frequently.

¹⁶ A Network Address Translation device translates addresses assigned within an organization to a different address when viewed from the Internet or another network. NAT is used for many purposes including dealing with the relative scarcity of IPv4 addresses on today's Internet and to intentionally hide the organization of networks within an organization. While NATs are useful, they tend to break connectivity for some kinds of applications.

Many current and future sources of data were identified as specific information that would assist our emergency response agencies with their response to calls for service. The networks we propose are “all-hazard”, “all emergency”. They are therefore agnostic as to which data travel over them; instead we care more about the form of data: real time or not, for example. Some examples of current and future data sources will help describe the need for a new network. They are listed in Appendix A under a number of categories. This is not intended to be a comprehensive list. It is intended to describe the diversity of data types.

The critical public policy point here is that the internetwork, and the emergency networks it links, should serve multiple uses and multiple users. It is inefficient and a detriment to interoperability to fund separate networks, for example, for health alerting separate from emergency medical data sharing, or a terrorism alerting network separate from the regular 9-1-1 network. All four of those should use the same basic network.

New data sources will arise continuously. Historically, creators of data sources invent them for their own purposes and are unaware that they are useful in emergencies by public safety. For example, many commercial buildings now have video surveillance cameras. They are installed for the protection of the employees and customers of the business, and run by the enterprise or its private security contractors. Emergency responders can make very good use of such capability but:

- There are no standards that would allow public safety to access them
- There are no registries of such systems that would alert public safety that they are available
- There are no methods for testing that when they are needed, the registry is accurate, the standards are adhered to, and the data will actually be available.

We must develop methods for identifying the availability of new data sources, provide leadership to develop standards for them so that they may be accessed¹⁷, and provide registration mechanisms so that their availability can be advertised where permissible by law or public policy.¹⁸ We must equip public safety with auditing tools and methods for conducting realistic drills to make sure data will be available when it is needed. This will require ongoing, national attention.

¹⁷ This is a particular challenge as the development of the data is usually done for non-safety purposes, and therefore is often well advanced before anyone thinks about standardizing it. Building plans are a good example. The National Conference of States on Building Codes and Standards, an initiative affiliated with the National Governor’s Association, is now trying to develop standards here.

¹⁸ Note that an emergency notification system is also an excellent form of “advertising” the availability of information sources to help respond to an incident, such as “just in time training” in streaming video, or instructions on how to handle a certain chemical.

Other issues which arise from new sources of data include: how is the new data logged? What media streams are recorded and what are not? Who can access them after an emergency and for what purpose?¹⁹ This could have profound implications for users. This is another good example of the need for new policy and protocol discussions.

5.2.2 Categories of data

There are several different categories of data. Some of these include: (a) Call data - data relative to a specific 9-1-1 call; (b) Location data - data related to a location that does not change from call to call, or incident to incident; (c) People data - data related to the person calling; (d) Incident data - data created during an incident that is shared among entities responding to the incident; (e) Service data - data related to the entities responding to the incident. Service area boundaries would be an example; (f) Response education data - data which assists agencies in responding properly, such as procedures, protocols, or training, and (g) data from decision support tools.

Each of these data is separate and distinct, and probably will be stored and managed differently. None of them are in any way tied to (determined by) the underlying network. We do not believe that it is appropriate in the future to tie transport of data to specific locations, storage mechanisms, or retrieval mechanisms. This does not mean that service providers should not be able to offer multiple services, but that logically, and operationally, they are entirely separate.

Thus, in the future model we describe call data is sent with the call. Location data is distributed. Some is stored in or with the GIS system. The rest is held in multiple data bases controlled by others, but available to any authorized response agency. People data is distributed. Most is probably stored in other systems that allow access by emergency agencies. Medical data would be an example. Response agencies would probably retrieve the pointer using the calling party's URI. Service data is located at the service provider (PSAP, Police, fire, poison control, transportation). Incident data is clearly stored in responder systems, but these are linked and dynamically updated. Responder education data and decision support tools (e.g. EMD or syndromic surveillance) may be located anywhere.²⁰

We advocate a uniform security model that would control who has access to and update privileges to such data.

¹⁹ HIPPA contains a complete exemption for the sharing of medical data during an emergency. The exemption does not apply to subsequent access to that information.

²⁰ Thus, there is no real equivalent of the current "ALI" system used by PSAPs, except for the simple translation of phone number to location that needs to be maintained for PSTN calls. None of the rest of the data currently found in the ALI would stay with that translation; it would be in the other databases.

5.2.3 Parties which must be linked by the future emergency network

An expansive definition of interoperability is required as the safety enterprise is very large indeed. It varies by incident type, but in every case includes both the headquarters and offices of the affected agencies and their staff in the field, not just one of those. It includes all levels of government: local, state, tribal and federal agencies. The internetwork needs to be designed so that there are effectively no barriers to adding appropriately authorized agencies, and it needs to have dynamic capabilities, both in users and in rights.

The internetwork should focus on organizations, not individuals. Organizations should be concerned about the systems that reach their members and staff. The reason for new systems is to strengthen and inform response agencies and their command structures, not disrupt them.

The following is a representative sampling of the types of agencies we envision that will be linked by the future network. It is not intended to be a comprehensive list. We have surely overlooked whole categories of participants. New members will no doubt be added as time goes by and other members may find that their needs have changed and may no longer need to be linked. As the scope of emergency response missions change in the future, more types of agencies may be identified requiring quick connection without putting the emergency network at risk. Such a dynamic situation can best be served by the principles stated earlier in this document. The connections must be standardized so that the connections, protocol, and procedures are uniform and seamless between each of the entities.

We offer the following non-exclusive list primarily to underline the point that the network is far more than the agencies of traditional “first responders”.

- a. Traditional public safety agencies: law enforcement, fire services, EMS, 9-1-1
- b. Citizens and businesses: connections between them and agencies (e.g. E9-1-1; truck fleet management systems)²¹
- c. Business safety providers (e.g. telematics, alarm monitoring systems; hazmat service providers)
- d. Hospitals
- e. Public health

²¹ 160 million cell phone subscribers and hundreds of thousands of trucks with GPS and communications systems are literally often the “first reporters” of incidents. Today they can provide exact location and verbal descriptions of incidents; in the near future they can provide pictures and other data, such as a direct report of a heart attack from a device worn on the chest. Thus the public must seamlessly be connected into the internetwork. This of course does not mean the public can access any part of the safety networks or determine the form and content of their communications to them; the exact forms of use of these connections are policy issues to be resolved by safety agencies, and the answers need not be uniform. For example, some agencies want to receive video with 9-1-1 calls in all cases if it is available; some may want such information only on their request.

- f. Emergency management
- g. Transportation
 - Departments
 - Modals (e.g. railroads, ports, trucking)
- h. Non-governmental organizations: Red Cross, Salvation Army, CERT, mountain rescue groups, etc
- i. National Guard
- j. US DOD
- k. Utilities, public works, recreation departments
- l. Media
- m. Schools
- n. Critical infrastructure companies

This does not mean every user has all the same rights to send and receive communications. As we note repeatedly, technical capability is different than policy. Rights are policy decisions that the internetwork must be able to implement – and those rights decisions must be made by the appropriate authorities, not the network configuration.

5.2.4 Current and future integration and decision support tools

By creating a flow of real time voice and data communications, the internetwork (and local and regional networks meeting the same standards) will enable, and create a demand for, integration and decision support tools.²² The quantity of information that can be developed in the course of even a small event can rapidly become overwhelming. Instead, these new tools can make suggested decisions, or other intelligent responses to inputs.

In the world of emergency medicine we are rapidly seeing the development of data from four sources: vehicles (telematics), personal medical information subscription services, oral conversations (e.g. with PSAPs), and on-scene personnel. Conjoining these data in new predictive, and dynamic, algorithms will provide a powerful new tool to emergency responders.²³

²² Until such data standards are created, parties will simply not invest in building these tools.

²³ For an extensive discussion of this matter, See articles on telematics, the Urgency Algorithm and related issues in Topics in Emergency Medicine, Vol. 26 No. 2, May/June, 2004.

In the hazmat world, the combination of substance and weather data, in a GIS tool, can produce extremely useful plume modeling. These tools can be programmed to produce additional emergency messages when pre-programmed triggers are reached.

Geo-spatial systems are another very useful integration tool. A common situational view on a map is often the easiest method of interagency data sharing. More sophisticated systems can produce alerts when mobile incidents occur within range of fixed resources (e.g. a hazmat spill near a school; a hijacking near a chemical plant). GIS systems are increasingly common, but they are also being deployed in haphazard, duplicative and incomplete ways. For example, often a municipality has a GIS system, the local 9-1-1 system has a GIS system and the local responder (police/fire department) has a GIS system and they are often all different, with different data, different layers, different accuracy, and different coverage and incompatible formats. We need more comprehensive planning and implementation of GIS, with more standards, and more uniform coverage.²⁴

5.2.5 The Need for Standards and Standardization Tools

Standards decisions must be made at the national (if not international) level. That should not mean "federal government" in most cases. Nor does it mean that we should nationalize safety. On the contrary, by implementing national transport and data standards, and creating similar interoperability enabling tools, we can increase local and state choice and flexibility in information use, response protocols and the like. But there needs to be a national consensus of the key stakeholder groups on a number of key items - discussed below.

5.2.5.1 Importance of standards

Fixed and mobile system interoperability requires standards, including standardized data sets. With these it is possible to achieve:

- Seamless service delivery between technologies and access networks for redundancy, reliability and mobility.
- Smooth evolution of technology and improved service through multi-technology/multi-band terminals and interoperable access networks and to a "common core" network providing uniform, comprehensive data entry and retrieval capabilities, data applications and multi-media service in the most efficient, effective, reliable and accessible manner.
- Forward and backward compatibility to allow for the introduction of new technology in a graceful or evolutionary manner without "leaving anyone

²⁴ The OGC is a consortium of public and private groups developing GIS standards.

behind" rather than in a "revolutionary" or uneven manner which could jeopardize some service to some users.

- Interoperability with public network technology, such as CDMA2000 and WCDMA/UMTS, in order to support plans for more effective participation of the public in their own safety as well as the continued utilization of public network access and features by emergency response officials as needed. This includes such new capabilities as a mobile emergency early warning system and a mobile emergency selective response system.²⁵

5.2.5.2 Standardizing data sets, protocols and interfaces

Effective emergency and homeland security functions require that different agencies from different professions be able to share information seamlessly across communications media. This will require ecumenical data sets. There is a consensus, which we support, that data should be in XML. There also seems to be an emerging consensus that we need standardized schema and data sets. While each profession may have terms which are unique to it, or unique understandings of certain terms, we can and should strive to have a common emergency language, starting with the terms which are shared: i.e. time, latitude and longitude, sender, type of message, etc. Such an initial effort is required to meet our recommendation of rapidly developing a limited set of common standard message sets.

There are multiple national data standards efforts in the different professional areas (e.g. law enforcement, emergency management, EMS, transportation), with little to no coordination between them. There is a great deal of repetition occurring, resulting in sometimes conflicting results. Until very recently there has been no venue or process seeking to bring these efforts together, much less the intensive program with federal support which is required.

The leading emergency standards efforts occurring now include: Project 25 Digital Radio Standards (APCO/NASTD/Federal agencies), OASIS (emergency management, led by EIC), IEEE (transportation), law enforcement community (Law Enforcement Information Technology Standards Council – LEITSC, the Global Justice XML Data Model, GJXDM)²⁶, XML.gov, TIA (ANSI) NHTSA/NAEMSP/NAEMSD (EMS), ATIS and NENA (9-1-1), OGIS (GIS), intelligent transportation (ITSA and ITE), APCO (radio and CAD), and ComCARE Alliance (vehicular emergencies and EPAD). There are probably others. In addition, there are a number of industry standards and standards efforts which can be used by emergency response, rather than reinventing wheels.

²⁵ "Mobile" implies access-independent mobility management functions through the core network as well as wireless.

²⁶ The Global Justice Information Sharing Initiative has recently invited some non-law enforcement and non-justice parties to participate. SAFECOM has recently invited non-traditional first responders to participate.

Another challenge is that we do not have years to follow the traditional route to standards creation. We need to follow a model of rapid development, deployment, real world use, and then improvement.

We must have a single process where emergency data standards for information that must be shared between emergency professions are coordinated and developed.

A final challenge is that emergency response agencies (or experts on their behalf) need to have a significant seat at the standards development table; indeed they will need to lead the efforts. State and local agency participation today is limited, and progress is slow, because it is usually volunteers who do the work. We need to democratize the process, and that means providing financial resources to directly support involvement of emergency responders in standards and protocol development activities.

We oppose the federal government setting standards itself, except as a very last resort. And we oppose re-inventing any wheels. We do however need a comprehensive, and intensive, emergency response standards effort, led by emergency response leaders with the resources to do it right. We propose that the FCC work closely with the executive branch of the federal government to fund a public/private effort to:

- Identify the groups and their standards efforts
 - Establish a coordinating committee with representation from all stakeholder groups
 - Create a shared website
 - Identify emergency response requirements
 - Reach consensus on a limited number of shared emergency messages²⁷
 - Determine what is available already from the private sector and prior emergency response standards efforts
 - Map the overlaps and identify the holes
- Facilitate action to address those²⁸

²⁷ One initial project to benefit all these message sets is developing a standard XML “emergency message header” to be used by all emergency messages for routing purposes. This is now underway, facilitated by the Disaster Management eGov Initiative (staffed by the Department of Homeland Security), and including a very wide range of emergency response organizations. This is part of DHS’s broader effort to facilitate the development of common emergency data standards as we suggest here.

²⁸ We strongly support the recent emergency data standards facilitation project of the Disaster Management eGov Initiative to accomplish exactly these goals, including establishing on-going communications between the standards efforts of the various emergency professional organizations.

5.2.5.3 Transport: TCP/IP

This issue has been resolved in our minds. We see no reason not to adopt this commercial standard, nor is there an obvious alternative.

The addressing standard of IPv6 is an open issue. While DoD has issued regulations mandating support of IPv6, there currently limited support for it in commercial equipment. Given expected lifetimes of public safety acquisitions, it would be highly desirable to mandate IPv6 now, but that might significantly limit available suppliers and increase costs in the short term. At the same time, it is clear that some aspects of IPv6, such as its larger address space and enhanced security environment, have great value for public safety. We advocate that all public safety systems be using IPv6, but should be fully backwards compatible with IPv4 systems.

5.2.5.4 Web services

We believe web services is the appropriate approach for most data interoperability. It particularly lends itself to the diverse communities and diverse data bases involved here. In addition to the agency registries discussed below, we need cached sets of authoritative data, and a web services Uniform Discovery and Data Integration (UDDI) of them. By representing data uniformly in XML form, we can provide a reasonable way to format it for display when no specific application is available to render it.

Extensive use of caching should be encouraged so that data is available close to the point of need, but is automatically kept current. By marking data with its expire date, caches can discard stale data without user intervention. When networks get isolated in disasters, the cached data may be the only data available. There is usually only one "authoritative" source of any datum. The owner of the data should explicitly replicate it in geographically diverse locations. The cache should refer to the authoritative source when it knows or suspects the data to be stale.

5.2.5.5 Publishing interfaces

Wherever possible, open standards should be specified and used. Vendors that wish to participate in procurements in the future should be required to use them, and to share emergency data. When proprietary interfaces are needed, they should only be selected when they are licensed to all competitors on reasonable, non discriminatory terms. Details about such interfaces should be published in way that allows networking between different equipment. Data should be self describing (i.e. XML with schemas and imbedded formatting).

5.2.5.6 Interoperability directories

Data cannot be routed without a directory of addressees and electronic addresses. Each user or vendor can have its own, which almost by definition ensures less quality, less comprehensiveness, and less accuracy. Rather than the inefficient profusion of single purpose directories that is growing today, we believe there should be a shared public/private utility. This should be a secure registry where authorized agencies enter their name, contact information, professional function, level of government, incident interests, the agency's jurisdiction, capabilities and interest area for each type of incident, and emergency data delivery address(es). Only authenticated and authorized users would have access to it on a non-discriminatory basis.²⁹

Such a directory will be most accepted and successful if it is a shared public/private effort. This will need to include an authorization system for agencies to register, run by the appropriate levels of government. We suggest that a portion of this registry be established to serve major employers (particularly those with significant public infrastructure or with assets which may be helpful in emergency response). As we note, there are many sources of data and facilities that are not normally thought of as emergency responders that are tapped when emergencies occur. Good examples would be a school bus system which might provide evacuation transportation, or an employer with a cafeteria available to feed a large group.

Agencies and localities will maintain supporting directories of their staff, public registrants for certain information, and the like. These can provide information as to local emergency agencies, and should be accessible by wireless devices.

5.2.5.7 Establishing authorization, roles and authentication

Linking networks will require a system(s) that will assure that only authorized parties may participate, as noted above, but we also must have a system that assigns them appropriate rights and roles, and that authenticates communications from them. There is no single agency or government that can do this. As in the registry discussed above, we recommend the development of public and private institutions for this purpose. (Some may already exist for other purposes; law enforcement has established similar systems for sharing criminal data using interstate networks.). These rules can be stored in a registry, or registry system, perhaps the same one which handles agencies addresses.³⁰

²⁹ Funded in part by a grant from the Department of Justice, the ComCARE Alliance is working with a number of other emergency organizations to develop such a directory, called the Emergency Provider Access Directory (EPAD).

³⁰ The DOJ Global Justice Information Sharing Initiative is currently addressing these issues for the law enforcement communities.

The rules need to be flexible so that they can be adjusted to conform to on the ground reality when disaster strikes. Of particular concern is the basic authentication mechanism for communications on the internetwork. We advocate uniform use of “public key” infrastructure for authentication credentials. To work, we need a “Public Key Infrastructure” for emergency response. We propose that an agency of the federal government designate a top level emergency response “certificate authority” (CA) which would authenticate a certificate authority for each type of responder that is large enough to support its own infrastructure. Each of these agencies would in turn authenticate a state level agency, which would authenticate each appropriate agency in their state. For example, the Department of Justice might establish a Certificate Authority for law enforcement, which might authenticate a Pennsylvania State Law Enforcement Certificate Authority. That CA would authenticate the Pittsburgh Police Department’s CA. The Pittsburgh Police Department would provide credentials to its staff. Each of these top level Certificate Authorities would “federate”³¹ with all the other top level CAs. In this way, any responder agency can verify the credentials of any response agency and any responder and make an admit/deny decision into an incident network authorization.

5.2.5.8 Enforcing standards

Merely having standards does not mean they will be used. Local, tribal, state and federal governments can speed the process of standards adoption by requiring their use by their vendors and grantees. Significant federal grants are being made today without such requirements. We recommend this be changed immediately to a system where grantees and vendors are required to adopt whatever is current available, and to incorporate new standard data sets as they are issued:

- For now: interoperable and seamless service using open architecture, IP, XML, web services, VoIP, SIP.
- For now: best efforts to incorporate existing standards and common vocabulary: Justice XML dictionary; OGC, NEMESIS, CAP, VEDS, etc.
- For now: other commercial standards of general applicability
- In the future: new standards designated by coordinating bodies with a particular emphasis on standards developed by ecumenical processes including all relevant emergency response agencies.

5.3 Redundancy and Reliability

³¹ “Federation” in this context refers to a technique where certificates issued by one certificate authority hierarchy can be accepted within another certificate authority hierarchy without requiring a single root CA to which all such CA hierarchies are subservient.

There is a common perception that today's emergency networks are both redundant and reliable. While that is certainly true in cases, we think there is much to be desired. The best results we have today are in mission critical radio systems. We need to spread the best practices for constructing reliable systems across the country in all emergency communications systems

5.3.1 Redundant connections to the networks

Network connections become more important as media types (e.g. voice, data, video) converge into broadband data networks. Agencies that rely on a single physical connection to critical networks are vulnerable to a whole host of conditions that could unexpectedly cut them off from those networks in their time of greatest need. We believe best practices, if not policy, require redundant physically divergent broad band connections using more than one system/carrier, and having access to more than POP with multiple points of access to the networks (e.g. cable, terrestrial radio, satellites).

Satellite communication systems provide extended network coverage to remote/rural areas without any other communications infrastructure, and rapid deployment of critical communications in major disaster areas. Since satellites used for this kind of communications are usually in high orbits, there can be transport delay introduced into the network when traffic flows over such links. Systems designers will need to be cognizant of the limitations and implications of possible satellite links on applications.

5.3.2 Use of Radio Spectrum

For years, public safety has wrestled with spectrum and technology issues that prevent one agency from having sufficient communications capability to perform its mission, and to interconnect with other agencies when mutual aid is involved. As we have learned from 9/11, cross agency wireless communication too often is not possible, and lives are lost because of it. There are a number of efforts underway to address this problem by reallocating channels so that agencies that need to communicate have some channels in common, and by deploying special purpose interchange devices that can provide some level of interconnection between otherwise incompatible systems. Over the longer term, we believe public safety would benefit greatly from greater interoperability and additional capabilities if more fundamental changes to communications systems were made to provide all agencies with sufficient bandwidth and allow any interconnections needed on scene when they are required.

Typically, the individual radios and networks of public safety private wireless systems use RF bandwidth in many small chunks (channels). While these systems do handle the voice traffic for a given public safety jurisdiction effectively, the data capacity of the channels is relatively small, measured in the thousands of bits per second. The larger spectrum problem for the 80,000 public safety agencies, having probably about as many

licenses, is that their spectrum is scattered across 11 bands, none of which (save 700 MHz and 4.9 GHz) has enough bandwidth to handle the types of data traffic proposed here. Additionally, channels in each band are separated in each spectrum planning region with incumbents spread as widely as possible in a geographic area to minimize co- and adjacent-channel interference, and to promote efficient voice system engineering designs.

It is our belief that public safety needs to dramatically increase the bandwidth a single device can support, moving from thousands of bits per second (kbps) to millions of bits per second (mbps). This bandwidth increase for an individual device does not mean that a given system would be able to carry less voice traffic. Instead, we believe that if a public safety radio had the ability to send data measured in mbps, such a radio could also easily handle all of the voice traffic needed as well. One way to address this is to clear a significant block of spectrum in a band with appropriate propagation to support both metropolitan and rural areas. Not only would this promote efficient systems with high data speeds, it would also eliminate the greatest impediment to interoperability: the 11 discreet bands now assigned to local/state public safety agencies by the FCC. The point here is that spectrum allocation needs to be rethought based on public safety's need for high bandwidth data sharing in addition to voice communications, while simultaneously and effectively addressing interoperability.

5.3.3 Mobile Ad hoc Networks (MANET)

The wired Internet is already a "mesh network". A few companies are deploying new wireless solutions that are able to turn wireless devices into nodes that can self-organize into their own wireless network and/or extend wireless service beyond coverage of existing infrastructure by relaying packets, or essentially hopping, through intermediate nodes. By being able to self-form and operate independently of infrastructure, these technologies may ease the problem of data interoperability at incident scenes. Wired IP network nodes, in particular routers within private intranets or the public Internet, have multiple (at least two, ideally three or more) connections to other elements in the networks, and the networks themselves have three or more connections to other networks in the internetwork, forming a mesh topology, rather than a hierarchical topology. We believe that wireless networks should also leverage this topology and make extensive use of so-called "mobile ad-hoc networking" technology - enabling self organizing, self healing, ad hoc mesh connectivity between endpoints. We specifically recommend against reliance exclusively on tower/endpoint systems - direct endpoint to endpoint radios can provide greater capacity and potentially better indoor coverage when a large number of people respond to a large incident. Careful thought and consideration should be given to the appropriate use of this technology, as this technology has yet to prove that it can reliably carry voice traffic, and therefore these networks may need to supplement emergency voice communication networks.

6 Major Considerations and Recommended Actions

The achievement of ubiquitous seamless voice communications and the promise of rich information³² are driving the evolution of emergency networks. Future networks will be packet-based networks that inherently support multimedia. Indeed, as a matter of high priority, and subject to quality of service principles with regard to mission critical wireless voice communications, we should move emergency communications to packet switching as rapidly as possible.³³ This will allow agencies to take advantage of the increasingly rich and diverse new information sources which are becoming available to emergency agencies, and thus extend this information to their staff in the field. Identifying, accessing and delivering these diverse voice and data communications will require significant effort, but will deliver significant added value.

These new emergency networks must be open architecture, using internationally standardized protocols, open API's and standardized datasets. Interoperability of equipment and the networks themselves is a fundamental requirement. The system should emulate the Internet's "hourglass" design whereby there are many ways to transport data, and many applications that use data, but there is only one transport protocol in the middle – the Internet Protocol (IP). This permits the system to provide the same services to a diverse user base over a wide variety of physical networks.

Like the Internet, we recommend the separation of transport from content, from applications, and from use policies and protocols. (See discussion of this point below).

Like the Internet, we believe this internetwork will provide robustness and redundancy. Indeed, it is important to recognize that access technologies are evolving faster than other technologies. We envision that each municipality, agency, region, state or tribe will have a variety of physical networks, some wired and some wireless. We advocate that each of these networks transport IP packets, and thus the services, applications and media streams available to one endpoint will be available to every endpoint. All media (voice, video, interactive text) can ride on packets. Of course the limitations of bandwidth, computing power, screen size, and other network transport and physical device constraints may mean that not every service behaves the same on every application. Thus, the capabilities of a small hand held wireless endpoint will vary from the capability of a high end wired desktop endpoint. Nevertheless, real time voice, video, text and data should be available to all endpoints seamlessly. We should transition away from special purpose emergency networks.

³² This paper tends to use the terms information and data interchangeably.

³³ Packet switching is today's near future. We must keep ourselves open to the next generation of fundamental technology.

It should be possible for each network to use both public and private networks for transport. Indeed, we recommend that emergency response devices should be capable of using both, so that a failure of a single network does not mean the endpoint is unusable. We think devices should be able to seamlessly switch between networks, rather than requiring people to carry multiple devices. By standardizing on IP transport, we think the costs of such systems should be modest; only the physical transport layer needs to be able to access multiple networks.

Unlike the Internet, security needs to be prominent in the design of the new emergency communications network from the beginning. Ubiquitous authentication, authorization, integrity and privacy of communications and data access will have to be built into every element.

We strongly believe that there should be no distinction between networks for “homeland security” and those for other emergency communications. The response community is the same for both. There will be different applications using different access methodologies to the internetwork for these different purposes – but the internetwork and the agencies participating in it are all the same.

The internetwork will encompass all communications transport forms. Subject to timing driven by the transition concerns and quality of service principles discussed above, we need to abolish the physical, organizational and policy separations between wireless and wireline communications. Similar distinctions between voice, data and video (and on-scene versus interagency communications) need to be removed, particularly for basic transport and interoperability decisions and policies. This is not to say that voice will not be distinguished from other types of data, far from it. The new approach will allow owners of networks to treat mission critical voice distinctly from all of the other types of data such a network would transport due to its critical importance to the public safety mission. Equally important, the basic internetwork -- the standards, rules, protocols, and facilitation tools -- need to be the same for all emergency agencies.

Federal policies or funding which continue to support these distinctions are reinforcing counterproductive silos.

We note the critical importance of another new factor: location.³⁴ Over and over we now see location of emergency response elements being raised in different emergency contexts. Every future network needs to consider responsibility for reporting the location of people and things which are on that network. In certain circumstances, location may be a trigger for communications.³⁵

³⁴ The very slow process of upgrading a small part of the future internetwork to accommodate wireless Enhanced 9-1-1 has provided many lessons for us as we face the much larger project with far more parties discussed herein.

³⁵ An example of this would be violation of a geo-fence.

In some wireless applications today, there may be trade-offs between web-based services and other alternatives when it comes to bandwidth. This could be an important factor for some wireless networks, at least until advanced compression techniques are developed and deployed.³⁶ We further recognize that these recommendations present a significant challenge to vendors and systems designers to deliver the needed level of security in the variety of end devices that will be common, especially those with limited compute power and battery life.

6.1 A Note on Transport v. Data v. Applications, and Tools v. Policies and Protocols

Most of the focus of our recommendations are on Transport (the movement of multi-media) – what is needed for packets of data containing voice, video, and other information to be ubiquitously available to emergency response agencies and their staffs.

That cannot really happen without agreement at some level on standardized emergency terminology and data sets, so we make some reference to the critical importance of those as well.

We do not address except in passing two other key aspects of emergency communications – and these should not be confused with the discussion of transport and data sets. These key areas are “Applications and Tools” and “Policies and Protocols”. Applications and Tools are the software and hardware that use the data: from radios to computer aided dispatch systems to algorithms that can identify threat patterns or the likelihood of death from a car crash. Policies and protocols determine which agencies and staff can send and receive which kinds of data, when and how, and what is saved. See Diagram 4.

The Transport and Data recommendations we make do not determine the answers in these two other categories, indeed we strongly believe that they enable a much wider degree of choices of applications and use procedures by local, state and other responsible officials on those key issues.

Standardized Transport and Data Sets means that vendors will be building for a national market, so that prices for emergency agencies should fall and choices should increase, exactly as has occurred in the commercial computer and software markets. Similarly, there should be significant effort to develop standards for the environment – software and hardware that the applications run on so that any application can execute on any device. Indeed we caution that many entities seem to be working on isolated

³⁶ In this regard we note the importance of the work of 3GPP2 on header compression standards.

“point products” designed to solve one part of the problem, but these applications make their own assumptions about the environment in which they execute and thus will be mutually incompatible with one another, and not integrate into the actual devices responders will have.

Just because data can flow everywhere to every agency and staffer does not mean they should. Policies for access and use need to be determined by the appropriate officials. Owners of networks and data should have the ability to control their use: what comes in and what goes out. The chain of command should be enhanced and empowered with more information, not confused by a Tower of Babel of new information inputs. Creation of such policies must balance the needs of national officials to obtain and inform the entire country and the needs of the local officials who create and maintain the networks.

We think it is critical to establish cooperative institutions to work out new Policies and Protocols (network and operational) reflecting these new capabilities. One example of such an institution that is already working in this area is the SAFECOM Program within the Department of Homeland Security. Our proposals provide the choice of sharing, which does not exist today; our proposals do not determine how and to what extent that sharing will occur.

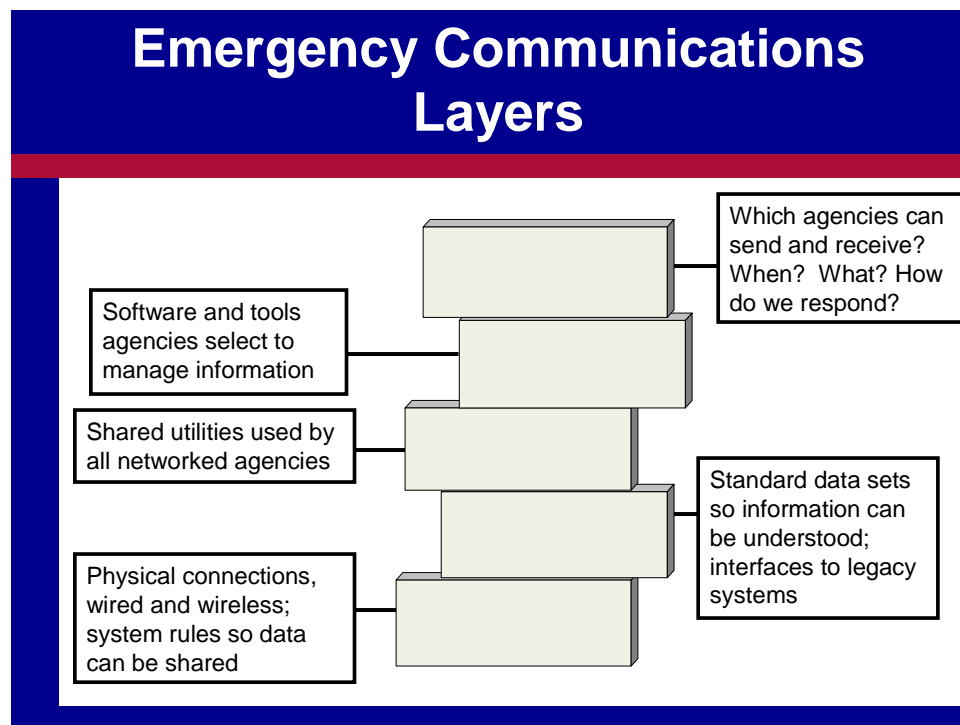


Diagram 4

Diagram 4: Transition to the Internetwork

It is important to underline that the initial step of linking tens of thousands of agencies together for basic interoperable communications in a packet switched network need not be a massive undertaking requiring many years. The ubiquitous Internet allows the sharing of emergency data among almost all emergency agencies today. The ultimate answer may involve different kinds of public and private IP networks to meet the particularly high requirements of mission critical voice communications, video and other similar uses

Nor do our recommendations either assume or require replacing most of the current safety IT/communications infrastructures – or requiring a flash cut transition. Indeed, the use of IP allows a far smoother transition to the future than past experience. As with the entire internetwork, physical and policy interfaces and rules are the key elements. For example, most computer-aided dispatch systems in use today can share data if an XML interface is built to the new data standards we discuss. Similarly, “converter boxes” are already being marketed which convert IP data into digital and analog radio formats and vice versa.

The nature of this broad and diverse emergency response enterprise means that adoption and change will come at different times. While interagency wired, satellite-based and other IP transport systems will make it much easier for rural agencies to close the divide with their urban counterparts, cost issues and topography will make deploying wireless broadband in rural areas harder. System design must thus assume that elements will evolve independently, new data sources will be identified and integrated, and new capabilities will be needed. Graceful migration, expansion and upgrade capability must be designed into these networks so they have both forward compatibility, and a high degree of backward compatibility.

6.2 *The Immediate Tasks*

Finally, while we cannot see a “flag day” conversion of existing systems to the kinds of systems we describe here, there are few networks in place in any public safety agencies that will meet the requirements we state here.³⁷ There are a variety of products and services that need to be developed, but there are no fundamental technical barriers to achieving this vision. However, there are a variety of challenges to overcome; these are primarily organizational and institutional.

- Agreement on this vision

³⁷ There are certainly some, but most are restricted to one agency in one area, or provide a restricted service to multiple agencies in one or many areas. This will change as more agencies begin deploying P25 systems.

- Development and/or adoption of voice data and media standards
- Assuring a baseline capability for all emergency response agencies, including the necessary wired and wireless bandwidth
- Developing a comprehensive authentication and access control infrastructure which will allow the security mechanisms advocated to be realized.
- Balancing decision making and governance between the various levels of government, and of our society: what are the local decisions? The national ones? The federal ones? The shared public/private ones?
- In an enterprise owned by thousands of parties, what are the common facilities and investments? Which entities will build and operate them?
- What part of these costs are appropriately borne by homeland security, by regular state and local safety expenditures, by other regular government expenditures (e.g. transportation), and by the private sector?
- What are the statutory and regulatory barriers to achieving this vision?³⁸

We believe there are significant cost savings to be achieved in mortality, morbidity, and operations from this new internetwork and the new services it will enable, but a significant initial investment is required. Consequently, we hope the Commission, Congress as well as other local, tribal, federal and state agencies will work together to provide sufficient funding to rapidly deploy the networks and related elements described here.

We believe that the federal government should ensure as rapidly as possible that there is voice and data interoperability along with a basic emergency messaging system between all emergency agencies. This should include the following specific capabilities:

- Broadband access by the 100,000+ emergency response agencies, and the 140,000+ schools³⁹
- Secure interagency voice and data communications, connecting those agencies, and allowing senior officials to immediately communicate with them and vice versa.
- Interoperable mobile voice and data communications for emergency responders in the field.
- A shared situational awareness tool (electronic maps)⁴⁰
- Shared, non-profit internetwork facilitation service utilities and processes to make them work, including:

³⁸ These range from a variety of FCC and spectrum issues, to outdated law enforcement rules in some states barring interconnection between law enforcement and non-law enforcement agencies.

³⁹ Due to the E-Rate Program and similar initiatives, a very high percentage of schools are already connected to the Internet with broadband access. Few to none are connected to any emergency networks.

⁴⁰ Both the private sector and the Disaster Management Program of DHS have been active in developing such basic tools.

- GIS-based registry of emergency agencies for message routing
- authentication registry⁴¹
- system rights management facilitation service utility
- Common messages standards for at least the following:
 - Alerting of agencies and the public⁴²
 - Real time incident status reports
 - Common coding of incident types and severity,
 - Response availability for an incident in progress
 - Request for assistance
 - Commitment for assistance
 - Status of commitment fulfillment
- Secure voice, data, and instant messaging between all responders, supervisors and dispatchers of all emergency agencies (i.e. intra agency staff communications)

The networks themselves should be decidedly non-hierarchical. Decisions on which persons and agencies receive which information, or can send which messages, must not be made by the underlying architecture - as they so often are today. However, the internetwork and the tools which it enables most definitely should not make the rules about their use. As noted above, just because any agency can now send a message to any other agency does not mean that is a good idea or should be allowed. Rather, explicit policy must govern which agencies are permitted to see what data. See Diagram 4.

Therefore, just as we hold detailed talks about technology, there needs to be a major parallel process of all the affected agencies to resolve what new Policies and Protocols are needed to take advantage of the internetwork and its tools, and to avoid abuses and problems. These new decisions must then be reflected in, and enforced by, the shared rules utilities of the internetwork. (See "facilitation service utilities" on the previous page and in Diagram 3.)

The goal is the establishment of a network characterized by fully integrated voice and high-speed data communications that delivers a broad array of data elements over a single local infrastructure with secure access to data and multiple foreign networks when appropriate permissions to such access are granted.

⁴¹ Work has already begun in this area. See, e.g., Imel, Kathy, "Study to Determine the Need for and Feasibility of Implementing a National IP-Based Public Safety Interconnectivity Authentications Process," May, 2004. Paper for the National Law Enforcement and Corrections Technology Center through the National Public Safety Telecommunications Council (NPSTC).

⁴² Note the formal approval in May, 2004 of the Common Alerting Protocol by the OASIS standards organization.

7 Outline of Recommendations

We summarize our recommendations here under each of the four questions posed to us.

1. Recommend whether IP architectures should be used for emergency communications, and, if so, how, and if not, what alternative should be pursued.

IP has emerged as the universal data language. As a consequence, we recommend its use. We recommend:

- Following the Internet model for a new “internetwork”, except institute a strong focus on security from the beginning.
- Increased research to identify and standardize as necessary the most appropriate air-interface(s) to support the robust transfer of packetized voice and data in a harsh wireless environment, recognizing that a family of waveforms may be required to best support different bandwidths.
- Expedited movement toward packet-switched communications networks, supporting voice and data services, both mobile and fixed.
- The architecture must support a multiplicity of secure, independently-managed IP networks using reliable but dynamic application-level connection models.
- IP platforms must allow emergency agencies preparing for, responding to, or mitigating emergencies to receive and operate with variable and increasingly rich data types while interoperating to provide emergency services.
- The architectures must support the full range of emergency events and responses, from day to day emergencies to mass disasters.
- The architectures must support emerging technologies, both those deriving from public requests for emergency service, and those generated from within the emergency response networks themselves.
- We believe an expedited implementation of IP architectures and systems will support an efficient migration path from the current systems while preserving the positive aspects of today’s solutions.

- We believe this approach will allow local and state emergency officials to gain access to new tools and new sources of information, while at the same time having control over access to their networks, and over their data.
 - In large part this involves supporting the development of interfaces from legacy systems to the new internet network so they can receive and export data, or convert digital/analog voice to IP.
 - Anticipated communications platforms must lay a foundation for future services that we cannot yet envision.
2. Recommend how methods for exchanging information between emergency agencies should be modernized.
- Accommodate a multiplicity of access methods, supporting emergency services requests from, and responses to, a broad array of emergency response disciplines, including but not limited to, law enforcement, fire, medical, public works and utilities, and the public.
 - Accommodate higher levels of interaction, managed situational intelligence, enhanced capabilities, and more comprehensive communication and coordinated response services.
 - Enhance interfaces that connect emergency agencies together and that support a multiplicity of communications types and services.
 - The internet network should focus on organizations, not individuals. Organizations should be concerned about the systems which reach their members.
 - Incorporate industry safety and engineering standards for reliability, availability, and survivability. Best practices require redundant, physically divergent broad band connections, e.g. telco, cable, wireless, and satellite.
 - Promote the highest degrees of security in IP and emerging future networks supported by proven network engineering and uses of sophisticated, but well known, security capabilities, such as two-way public key cryptography scheme that achieve authentication of two participating computing platforms and encrypting their communication to prevent unauthorized access to private information.

- Include communication security mechanisms such as Secure Sockets Layer (SSL), TCP/IP interfaces using Public Key Infrastructure (PKI) exchange of digital certificates to verify client and server identities.
 - Adopt network and application layers that support clients – such as PSAP 9-1-1 CPE and other systems – dynamically identifying available hosts.
 - Promote the implementation of application message layer protocols to achieve communications availability through redundant network paths, redundant network elements, and flexible application messaging interaction scenarios – irrespective of the content of the data.
 - Routing decisions in the networks themselves should be decidedly non-hierarchical. Decisions on which persons and agencies receive which information, or can send which messages, must not be made by the underlying architecture or tools. Those are policy issues to be implemented by IT tools.
 - Recognize that Transport and Data Standards enable new Policy and Protocols. They do not decide what those should be. There needs to be a major parallel process to set new policies and protocols to take advantage of the internetwork and its tools, and to avoid abuses. These must then be enforced by the shared rules utilities of the internetwork.
3. Recommend architectures that will allow emergency agencies to exchange voice, text, pictures and other types of data.
- Implement communications architectures that are unconstrained by limited messaging capability, dedicated server models, fixed point-to-point communications, legacy design choices, and a lack of expandability.
 - Apply extensible message sets to allow emergency service providers to participate in emergency response functions or provide a gateway function to external processing elements that may provide the native interface to additional service providers.
 - Improve communication and information delivery, including higher interaction models with varying originating device types

- Encourage the development of enhanced algorithms for retrieving available and relevant emergency information from diverse data systems, and providing decision support.
- Assure advanced selective routing, call routing, and call transfer logic integration within diverse communications technologies.
- Adopt web services systems so that there is dynamic access to information in multiple data bases of multiple parties.
- Implement flexible authorization systems. Agencies must be able to decide whether or not to share their data, and then to “tag” data to have the internetwork enforce their rules on sharing it. This will help overcome opposition to interoperability.
- Similar systems must allow the implementation of owner-determined priorities on the use of their networks (by user, type of use, incident type, etc)
- Implement a nationwide routing registry or registries. Agencies need to be able to advertise availability of services, events and data. Agencies need to be able to register to receive incident data, expressing what incident information they want, for what geographical area, and how and where they want it sent to them. There must be a trusted process to authorize entries and use of such registries.
- We need a common system that assigns agencies appropriate rights and roles, and that authenticates communications from them. As with the routing registry, we recommend the development of shared public/ private institutions for this purpose.
- Launch an intensive coordination and rapid deployment effort to develop common data sets, and a set of common emergency messages. Foster standardization of bi-directional message sets. Require the use of XML and such standards in all procurements and future development.
- Government should not set standards itself; it should provide the resources to ensure that professional response organizations can play a leadership role, and that there is an intensive public/private standards effort. Standards themselves should be set by internationally or nationally (if appropriate) recognized standards organizations such as IEEE, IETF, OASIS, ITU and TIA.

- Implement message sets that are supported by established technologies and protocols such as TCP/IP, HTTP, SSL, XML, and SIP/SDP.
 - Promulgate infrastructures that support the ability to plug in additional data services, multi-media, and voice.
4. Recommend the communications capabilities needed to exchange relevant information in a uniform and seamless manner with the Department of Homeland Security and other agencies in major disasters and for terrorist attacks.
- The emergency systems we describe are the central nervous system of the National Incident Management System (NIMS) and a modern Incident Command System (ICS).
 - The primary way for Homeland Security agencies to receive appropriate data is to have an effective day to day emergency system which can be tapped into during a national emergency. The wrong way is to create “homeland security” networks or applications in their own silos.
 - An effective day to day system allows the installation of “sniffer” systems to report deviations from normal patterns of 9-1-1 call types, Emergency Medical Dispatch incident definitions, EMT/Emergency Department primary complaints. This is only possible with an automated, electronic emergency response system.
 - When there are national emergencies, external officials can “listen in” to otherwise local networks. They can register for incident notifications like other agencies.
 - This approach allows commanders to manage resources from different jurisdictions and diverse disciplines responding to, managing and mitigating major events while serving as a physical or virtual command center.
 - Manage first responder call out notifications and the initiation of 9-1-1 in reverse notifications to the public.

- The federal government should ensure that there is a basic emergency messaging system and data interoperability between all emergency agencies as rapidly as possible. This includes:
 - Agency broad band connections
 - Secure two way data and voice interagency systems
 - Shared electronic maps and GIS capability generally
 - Shared utilities including an agency routing directory, and authorization, authentication and rights systems
 - A set of common emergency messages
 - Secure instant messaging between individual response staff

- Sharing of networks should be encouraged to reduce costs.

8 Appendix A – Samples of Data Types

During our discussions, many current and future sources of data were identified as specific information that would assist our emergency response agencies with their response to calls for service. The networks we propose are “all-hazard”, “all emergency”. They are therefore agnostic as to which data travel over them; instead we care more about the form of data: real time or not, for example. Some examples of current and future data sources will help describe the need for a new network. They are listed here under a number of categories. This is not intended to be a comprehensive list. It is intended to describe the diversity of data types and to underline the point that the emergency networks of the future should not be developed for specific professions or incident types. There may be specialized applications for handling data in those circumstances, but the underlying network and standards should be shared. The SAFECOM Statement of Requirements issued in 2004 provides a more detailed list of incident and data types.

8.1 *Real time data from the public*

- Ability to transmit digital pictures (either digital camera or cell phone camera) from a concerned citizen to field units (through ECC). Real time video from mobile phones is now becoming available and should also be able to be sent to responders.
- Hazmat alarms from fixed facilities which should include location of facility and hazmat material location, temperature information (including heat if present and how high), name of material (amount and packaging) with a cross reference with products and chemical names and product sheets, live video feed to responders and PSAP, and any alarm triggered equipment response at the facility such as flushing, ventilation or release of cleanup or anti hazmat system.
- AED activation info when available and if patient is monitored at home, all data on patient including past and current condition and any allergies.
- Ability to automatically receive power outage information in PSAP and at the field level consisting of a map showing coverage of the area affected.
- Remote access to interior video surveillance cameras by exterior responder units.

8.2 *Real time data from private sector providers*

- Telematics information (for example On Star) to include the number of occupants, speed upon impact, position of the vehicle (roll over), if the air bags were deployed, load information (hazardous materials, what kind and how much and how packaged), live video feed, connection with DOT cameras, live feed with updated information, and ability to transfer the video feed and patient information including current vital signs to transport unit (ground or air) and medical facility.
- The ability to map the location of a missing at-risk person (Alzheimer patients), missing children, and probation/parolees with electronic monitors.
- Burglary alarm call information should include location and facility information. Receive live feeds from a camera inside the structure in both dispatch and the field during the course of the event (from activation till closure of the call)
- An electronic manifest showing contents of a vehicle involved in an accident (see first bullet) w/connectivity to electronic DOT Hazmat Response Guide information in both the field and dispatch.

8.3 *Real time data from other response agencies*

- Transfer Phase 2 wireless location/mapping information to field units, and to other agencies.
- State DOT road sensor information to PSAP and responder including road conditions, speed sensors, and live video feed.
- Local/regional tornado/hurricane or weather related siren information including location, direction and speed of travel, and severity.
- Local/regional Homeland Security information or Amber Alert information including maps, photos and pertinent data.
- Video feeds from law enforcement helicopters, including infrared/heat information to both responders and the PSAP.
- Real time video feeds from field to PSAP, Incident Command Post, etc.

8.4 *Integrating data from multiple sources and forwarding it to agencies*

- Aircraft information to include passenger numbers, cargo manifest, fuel amounts, speed at impact, video feed from the scene of event to PSAP and responding units while en route, plus the ability to forward all of that data to a medical facility.

- Fire alarm information should include map of building/facility with marker of location of water flow info or where smoke detectors were activated (how many and location), location of heat detectors and actual temperatures (real time) being received , and any hazardous materials information associated with the facility including its location, type and amount, and associated DOT HazMat Guide information

8.5 Real time data between agencies and their staff in the field

- GPS information (x,y,z) of field units both vehicles and individuals, and the vital sign information of the personnel. (This info should be available to be accessed as needed.)
- Access to GIS, hazmat, MSDS, building floor plans, unit locations, etc, In general, any information available to field staff should be available to HQ staff and vice versa in real time.
- Wireless access to situational awareness/incident management software to incident commanders and emergency managers.

8.6 Non-real time data from stored data bases

- Modeling of traffic, plumes, other based on past events
- Just in time training videos
- Instructions on handling different types of emergencies

8.7 Interactive data

- Intelligent alerting systems for individuals
- Response actions by agencies automatically transmitted to others registered for those.