NRIC VII

December 2005

FOCUS GROUP 1D

Communication Issues for Emergency Communications Beyond E911

Final Report – Properties, network architectures and transition issues for communications between emergency services organizations, including PSAPs

1 Results in Brief

1.1 Executive Summary -- The Emergency Communications[1] Internetwork

Emergency responders are asked to do one of the most important jobs in our society with communications and information technology that most businesses have moved far beyond. Everyday emergency responders step into harm's way without information that would help them, and without the tools to stay in touch with their colleagues; commanders in headquarters and in the field are asked to operate without the most modern information technology tools, and the information sharing from and to a wide variety of emergency and non-emergency sources of information those tools could provide.

A critical weakness of current American emergency communications systems is that agencies are generally 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[2] between emergency organizations of all kinds. With the right systems and tools, there could be faster, more informed and more efficient emergency responses.

Focus Group 1D sees the solutions in two complementary areas: technology and institutions (including the leaders in them). This report focuses on the former, but the latter is probably more important. The effective future emergency communications systems need to be linked in an "internetwork"[3] – a set of policies, tools, interfaces and standards that connect securely the multiplicity of local, regional and national wireline and wireless networks. It will enable modern, integrated information capabilities to support local, regional and national emergency needs. Some could call this a system of systems.[4] The following Diagram 1 is an illustration, from one perspective, of this

[1] The terms "emergency communications", "emergency organizations", and "emergency responses agencies" are used instead of the traditional term "public safety". This is done deliberately because these terms encompass a significantly broader scope of parties and organizations than the more traditional terms "public safety communications." This paper, and we believe proper policy, recommends a seamless system connecting the public to agencies and organizations of all kinds that support emergency response, and those organizations to each other. The definition of "agencies" used herein 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. Similarly, we see Public Safety Answering Points (PSAPs) as critical nodes in emergency response networks, but architecturally no different than other emergency organizations, as shown in Diagram 1.

[2] This paper tends to use the terms "information" and "data" interchangeably.

[3] This unfamiliar term is used to make two points: (a) a 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 Focus Group 1D does 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 (and applications that ride on them) into a seamless whole, rather than replace them.

[4] "System of Systems." Emergency 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

"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 local, state, federal and private networks of wireline and wireless that will connect agencies and emergency responders in various ways. These are more fully displayed in Diagram 2.

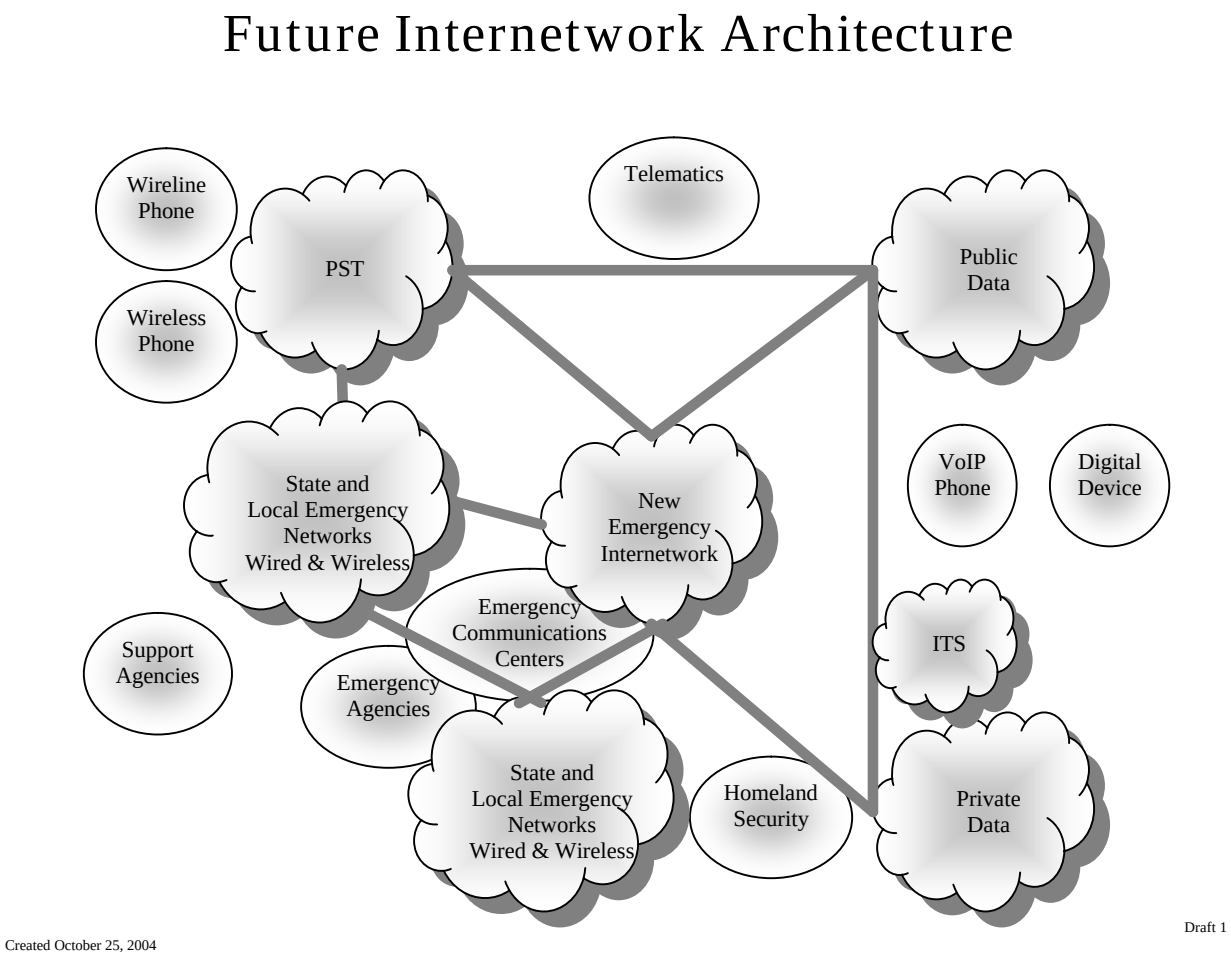


Diagram 1: Future Internetwork Architecture

Homeland Security. One driving force towards achieving this goal is concerns about homeland security. The Department of Homeland Security now requires that all recipients of its grants comply with the National Incident Management System (NIMS), and meet a specific list of Target Capabilities. The Focus Group 1D recommendations are entirely consistent with, and should be the central nervous system of NIMS and a modern Incident Command System (ICS). Indeed, communities simply cannot meet a large number of the key items on the DHS "Target Capabilities List" without interoperable voice and data communications systems of the kind this report advocates.

---

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.

But the only viable way for organizations responding to homeland security threats and events to receive appropriate data is to have an effective day-to-day emergency communications system that can also be used in large scale emergencies. The wrong method is to create "homeland security" networks or applications (or generally any other single purpose emergency communications system) in isolation.

The Safety Enterprise. Policy makers and practitioners should regard all emergency agencies, both public and private, as an overall "enterprise," rather than a collection of separate entities, or subsets of them[5] -- the multiplicity of unconnected and isolated "silos" that exist today. A complete enterprise perspective will give planning and policy making the 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 separate agencies.[6]

Some of these have now developed interoperable wireless networks for the public safety agencies in their communities; others are devoting enormous efforts to achieve that critical goal. Roaming-capable radio interoperability via the TIA-endorsed P25 standards process 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's SAFECOM Program and grant funding. The current scope of roaming interoperability allows users from any jurisdiction to respond to incidents in other jurisdictions and to be able to use their own devices for voice communications. However, for data communication interoperability the current scope only specifies a common wireless interface. Only a much smaller number of communities are pursuing application layer data interoperability between their emergency agencies, much less with the public in general. There is no similar federal program for this purpose.

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, major attention must be devoted in the near term to develop the cooperative institutions to provide the policies to govern this new interconnected system.

---

[5] SAFECOM is working on an enterprise architecture for first responder wireless communications ("public safety communications"). There is a federal enterprise architecture effort (designed to encompass all federal IT activities). There are a number of state enterprise efforts (encompassing all state IT activities). There is no comprehensive emergency architecture effort of the breadth we recommend now being undertaken.

[6] Focus Group 1D assumes that there are about 120,000 organizations that 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.

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 organizations and responders from many different areas including national agencies

This emergency internetwork will empower emergency agencies to have far more control over information flow and use than they have today. It should save them time and money in daily use. Diagram 2 provides a more detailed view of the internetwork that Focus Group 1D envisions. It shows how wireline and wireless networks of different levels of government and agencies can interconnect with each other and the public.

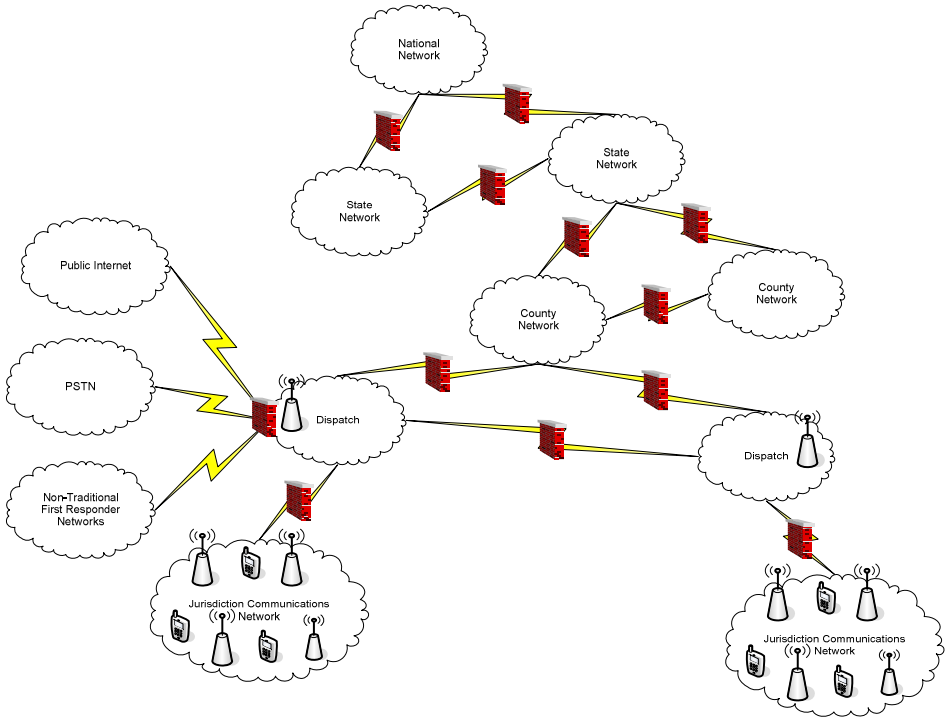


Diagram 2: Interrelationship of Networks in the Internetwork

Summary of Vision and Recommendations. This paper discusses Focus Group 1D's vision of emergency communications by 2010. That vision is summarized as follows, and partially illustrated in Diagrams 1 and 2 above, and Diagram 3 below. The vision and

recommendations summarized here are discussed in detail in Section 5, according to the five overall "building blocks" shown in Diagram 4.

(1) Emergency response organizations, their staff, and the public should be able to access the information they need, whatever the source, when they need it, in a usable form, using whatever electronic communications device they have.

(2) Interoperability is not only about first responders "talking to each other"; it needs to include inter-organizational data communications. Ultimately, distinctions between voice and data will disappear, and the internetwork will move information seamlessly across wired and wireless platforms.

(3) The current "siloed," agency-specific systems and applications need to be replaced by shared interoperable ones, or upgraded with interfaces to allow interoperability.

(4) The most important barriers to this interoperability are institutional and professional, not technical. Today's system of thousands of independent islands needs to be replaced by a cooperative, interdependent system of information sharing.

(5) Even with such cooperation, these changes will not come about without strong national and state leadership, coordination, and funding.

(6) The corollary is that the most important success ingredient to achieve this vision is empowering emergency response professionals. Most of this report is about information technology, but success will only come from enabling major operational and cultural changes in how emergency services are managed -- when responders can be informed by significant new data sources and equipped with tools to manage them.

(7) A key part of allowing new data sources to inform responders, rather than overwhelming responders with data, is the development of an array of new decision support and information management tools.

(8) A single, interconnected Internet Protocol system should be used for all emergency communications, connecting a wide variety of agency-run and public networks, both wireline and wireless. Focus Group 1D calls this an "Internetwork" to emphasize that this group does not believe a new physical network is needed. It is a system of systems approach.

(9) The same network infrastructure, standards, protocols and basic applications should be used during all emergency operations, small and large. Shared

networks (for all emergency agencies) should be encouraged to reduce costs and improve interoperability. Systems built for a single purpose should be discouraged.

(10) Significant new federal funding is needed, focused on building these shared interoperability capabilities.

(11) Emergency response agencies need more spectrum, both the narrow band spectrum contemplated from the Digital Television transfers, and a new contiguous set of bandwidth for wireless broadband use.

(12) Data and networks should be organized in a distributed, not a hierarchical, architecture, embracing a multiplicity of communications pathways and methods based on the Internet model. Wherever possible single points of failure need to be eliminated.

(13) There should be a new set of "Facilitation Services"[7] cooperatively-managed by the emergency response communities themselves to provide common coordination and facilitation functions for cryptographic certification, authorization policies, message routing (e.g., directory), and resource discovery. Access to network and information resources (e.g., 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. Facilitation services should be developed and managed by the emergency response agencies themselves.

(14) Every emergency organization needs redundant broadband communications.

(15) Multiple methods of data communications need to be encouraged. Single points of failure and the required use of proprietary systems should be strongly discouraged. Diagram 3 demonstrates several methods of data sharing, and the use of common Facilitation Services, specifically:
   a. Direct agency to agency communication with no intermediation
   b. Use of a service where agencies post data to a server ("push"), and/or can poll from one when they wish ("pull")
   c. Agencies can access common "facilitation services" directly
   d. Agencies can use intermediary providers to deliver messages, and/or enrich them. These providers can decide whether or not to use the "facilitation services"

[7] See Section 5.4 for definition and discussion of Facilitation Services.

(16) 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.

(17) XML-based data elements and message structures for interchange of common emergency-related information across professions should be defined. Where these do not exist, they should be developed by open processes of all emergency agencies, not by specific emergency sectors.

(18) All emergency communications should be protected to ensure privacy and integrity of the communications.

(19) There is a set of core application-layer protocols that should be specified, namely for event notification, session setup, resource discovery, email, IM, and similar functions.

(20) To accomplish this vision, action is required on a list of "Immediate Tasks" identified in section 6.3, as well as longer term planning.

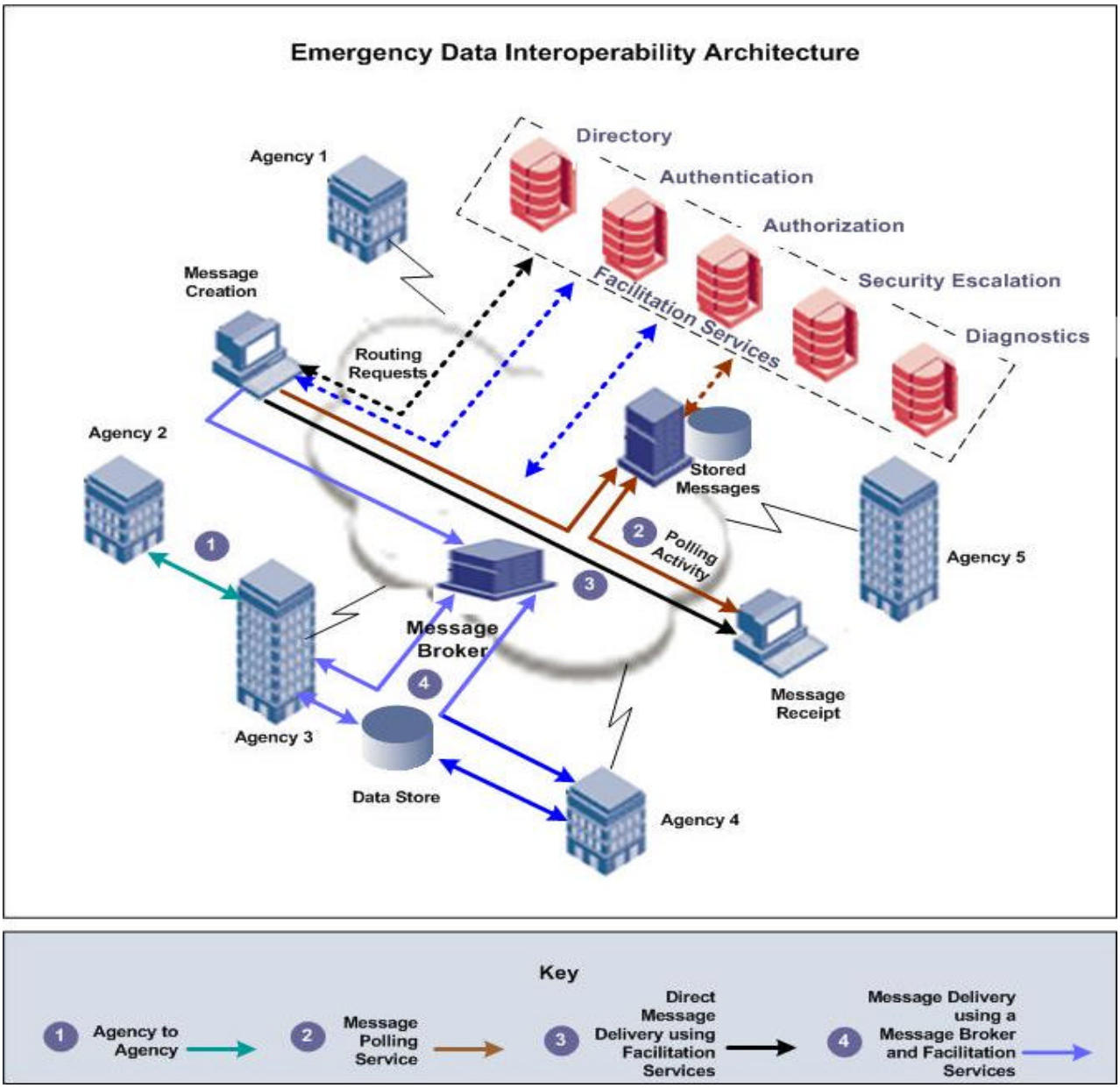


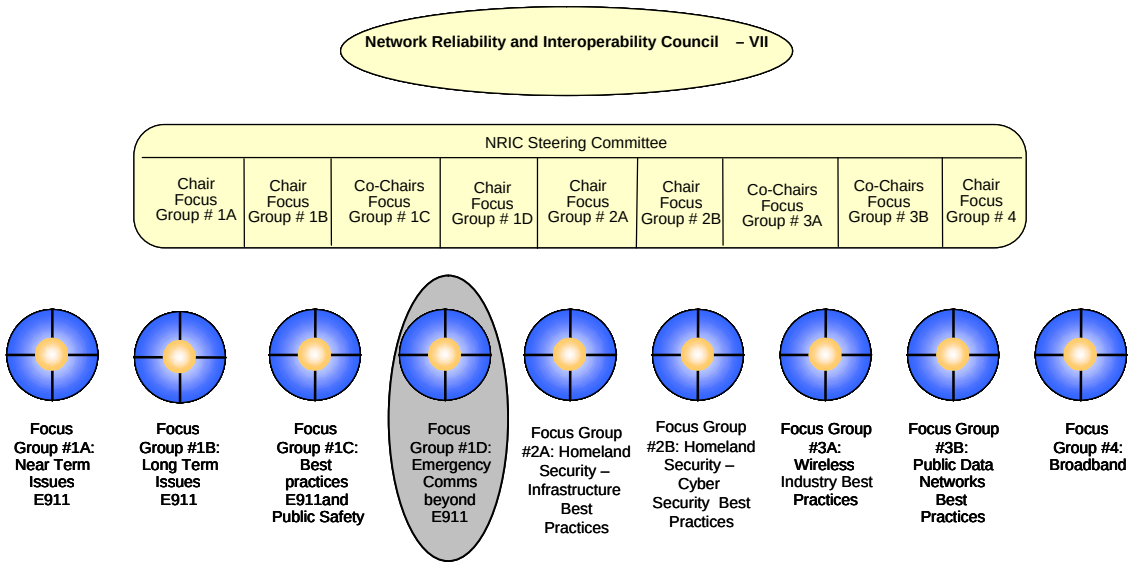
Diagram 3: Emergency Data Interoperability Architecture: Many Choices

2 Introduction

This final 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. In other words, the emergency communications system in which 9-1-1 centers are key entities, but only one of many entities responsible for responding to emergencies.

Structure of NRIC VII

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



2.1 Focus Group 1D Team Members

Focus Group 1D consists of the members 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
Sukumar Dwarkanath	COMCARE
Kamil Grajski	Qualcomm
Mario DeRango	Motorola
Dale Morgenstern	AT&T
Charles Werner	Charlottesville (VA) Fire Dept.
Brian Rosen	Neustar
Darryl Foster	Cox Communications
Amarjit Deol	Nortel
Robert Schafer	MCI
Tom Steele	IACP
Stuart Goldman	Lucent Technologies
Douglas Rollender	Lucent Technologies
Stu Miller	Intrado
Marilyn Haroutunian	Sprint Nextel
Charles Hoffman	NTIA
Michael J. Mangini	Plant Equipment
Marilyn B. Ward	Orange County (FL) Public Safety
Percy Kimbrough	SBC
Marty Feuerstein	Polaris
Bob Dressler	Polaris
Marilyn Handy	NTIA
John Powell	NPSTC
Andrew Thiessen	NPSTC
Rick Jones	NENA

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 organizations and personnel that is beyond communications between PSAPs, and between the public and PSAPs. This includes the identification of architectures that will be able to transmit the needed information about emergency events to all persons and agencies that need it, and to aid in coordinating emergency services activities.

3.2 Scope

This document addresses the 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.[8]

2) The Council shall present a report that recommends the network architectures for communications between PSAPs and emergency service personnel[9] 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.

3) The Council shall present a report describing the transition issues for the recommended target architectures along with its recommended role for 911/E911 in major disasters and terrorist attacks.

4) The Council shall present a final report describing the properties of the target architectures for PSAP to emergency services personnel communications, the recommended network architectures, the transition issues, and a proposed resolution of these transition issues along with a time frame for their implementation.

3.3 Methodology

The Focus Group members participated in a large number of conference calls and face-to-face meetings to develop the recommendations in this report. They consulted with emergency organizations not part of the Focus Group, including a formal meeting where a broad group of emergency organizations were invited to comment on the recommendations of the Focus Group's interim report. Additionally, the report was cross-referenced with the recommendations previously made by Focus Group 1B to ensure consistency across these two related Focus Groups.

4 Background

4.1 The Changing Face of Emergency Communications

Traditional emergency communications have been voice-based: telephone and radio. Until recently, "emergency data" was generally limited to entering information into an agency-specific computer and records management system during or 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

[8] The Focus Group decided that most requirements needed to be met long before 2010.
[9] The Focus Group decided that organizations and agencies were the appropriate subject of its focus.

(e.g., police and fire mobile data units communicating with their headquarters, and then to foreign databases for limited purposes, such as NCIC). An FCC-sponsored study by Professor Dale Hatfield pointed out the inability of current PSAP technologies to accept external, much less dynamic, data.[10] 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 paper.[11]

Until recently, discussions of emergency communications interoperability have been generally confined to radio use in response to a localized incident. This focus has been on the traditional public safety ("first responder") agencies and their use of wireless communications systems. While those issues are critical and must be resolved, information sharing and interoperability must be addressed in their full scope, including inter-organizational communications using all forms of communications.

New technology, demands of homeland security, and new commercial products which produce data for emergency response (e.g., Enhanced 9-1-1, telematics), and the recognition that multiple data sources exist that could assist in emergency response are forcing change. A wide variety of electronic data sources that need to be handled by emergency response officials, or could improve emergency response, are becoming available. Many of these can be found in the SAFECOM Program requirements paper issued by the Department of Homeland Security.[12] Others are described in Appendix A of this report.

The distinction between interagency communications and communications with the public also needs to be removed. For example, over 180 million US wireless subscribers are a key source of information for emergency agencies.

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 often resides elsewhere. It is getting increasingly difficult to handle events requiring multi-agency responses, particularly large incidents, efficiently or accurately with voice communications alone[13] or with only data communications from a command center to its staff at the scene. This is equally applicable to public alerts and warnings (e.g., Amber alerts). 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.

---

[10] See Hatfield Study of E9-1-1 for FCC, 2002.
[11] See Meer and Nelson, Submission to ATIS, June, 2004
[12] See www.safecomprogram.gov.
[13] See 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.

4.2 Users

The emergency response internetwork needs to accommodate a wide range of government agencies, non-profits, private sector businesses, and the public. Hereafter, the term "emergency agency"[14] is used throughout this paper, but it is intended to have a very broad meaning. The users of the internetwork will be any and all organizations that improve the safety of the public by being able to exchange information before, during or after emergencies. Policies governing network access and use will vary among these groups depending on their status and circumstances, but they should be part of the same internetwork.[15]

4.3 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, which 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 interconnections between government networks and public networks are needed in order to do the kinds of things envisioned 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.

[14] 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). That is a useful policy and/or protocol distinction, but Focus Group 1D believes it should not be used for designing the appropriate architecture and technical capabilities.

[15] See Section 5.1.4 below for discussion of the importance of separating technical interoperability from policies that govern actual usage.

4.4 Geography

The primary focus of public and private efforts to develop modern emergency communications 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. Those leading the development of emergency standards for the US 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, providing efficiencies that may be passed through to emergency agencies.

4.5 Purpose

It should be a high national priority 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 outcome. A fundamental principle for the future is to empower emergency staff. This future needs to be practitioner, not vendor, driven. Information needs to be provided where it is needed, when it is needed, to the people and agencies that need it, as authorized. 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.

This would empower the appropriate chain of command with new tools and capabilities. To accomplish this goal, the system needs to be highly flexible, with mechanisms which allow very different information flows depending on the needs of the moment.

One important aspect of emergency information sharing is that for the first time end-to-end incident records can be created, which will provide a serious basis for research, relatively inexpensively, because this data collection will be a byproduct of daily use.

4.6 System Reliability and Design: Copying the Internet Model

The future system must be extremely reliable. The two primary methods of achieving reliability will be (1) the redundant nature of the internetwork[16], and (2) multiple access methods to the internetwork from participating agencies. In addition, data should be distributed (i.e., not single large databases, but multiple smaller ones), replicated (i.e.,

[16] See footnote 3.

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

Packet switching is inherently more efficient than today's circuit switched networks. It is far more likely to allow completed communications in a high usage situation (although the quality of communications may be degraded).

The Internet is an extremely useful educational source, both in positive and negative terms. It has taught us a great deal about what to do and what not to do in developing architectures for future emergency communications. It has generated a host of best practices. Except for the lack of attention that was paid to security until recently, Focus Group 1D believes the Internet is the architectural model which should generally be followed for future emergency communications, with the caveats discussed elsewhere in this paper.

- **Separate transport from applications**

Emergency agencies have had a tendency to intertwine transport protocols and methods with the data they are carrying. Thus, there is a PSAP network for location data, and another one (i.e., law enforcement) for crime information. There is a third for major public warnings (i.e., EAS). One of the reasons for the great success of the Internet was the complete separation of transport and applications, and agreement on one transport protocol: Internet Protocol. As a result, applications, tools, and data sources have exploded. Focus Group 1D proposes to use this model as well as many of the Internet protocols.

- **Separate applications from types of data**

In a similar way, Focus Group 1D believes the most progress can be made most efficiently if applications are separated 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 interfaces and common message structures should be used.

- **Common directories**

For the Internet, a limited number of private and/or non-profit entities provide a quasi-governmental function in providing addressing. That model should be followed in the future as well (see discussion of Facilitation Services in Section 5.4).

4.7 System Interoperability

4.7.1 Defining Interoperability

"What is communications interoperability?" The SAFECOM Program says:

> "In general, interoperability refers to the ability of public safety emergency responders to work seamlessly with other systems or products without any special effort. Wireless communications interoperability specifically refers to the ability of public safety officials to share information via voice and data signals on demand, in real time, when needed, and as authorized. For example, when communications systems are interoperable, police and firefighters responding to a routine incident can talk to each other to coordinate efforts. Communications interoperability also makes it possible for public safety agencies responding to catastrophic accidents or disasters to work effectively together. Finally, it allows public safety personnel to maximize resources in planning for major predictable events such as the Super Bowl or an inauguration, or for disaster relief and recovery efforts."[17]

The Focus Group 1D vision of interoperability extends the SAFECOM vision, and uses it as a fundamental building block. Focus group 1D agrees with SAFECOM's vision and this report contains a series of proposals for achieving this vision in areas that have not been the traditional focus of SAFECOM. Focus Group 1D identifies the Internet Protocol as an enabler, and recognizes the importance of voice, data and video communications in achieving this vision of a truly heterogeneous and seamless Emergency Services internetwork. Focus Group 1D recommends that emergency services decision makers at all levels of government recognize the reality that there will never be (nor should there be) a single emergency network. Instead, this paper describes a network of networks, a set of policies and tools that allow effective communications across a series of separate but interconnected physical and virtual networks.

Focus Group 1D extends the SAFECOM definition to cover a significantly broader community than the traditional public safety (e.g., first responder) agencies, more than doubling its size (to around 120,000 independent organizations). What this paper calls the "emergency response community" includes both the traditional public safety agencies and the entire set of public and private organizations that need to share information in emergencies of all kinds. Thus, it includes not just law enforcement, fire services, EMS and 9-1-1, but also emergency managers (and their emergency operations centers), hospitals, clinics, public health agencies, transportation, public works departments, utilities, elected officials' offices, other government agencies, and private entities from infrastructure providers to telematics companies.

[17] http://www.safecomprogram.gov/SAFECOM/interoperability/default.htm

Focus Group 1D's focus has been on the architecture of the overall internetwork that can tie all of these organizations together, and specifically, the higher layer constructs required for true application and data interoperability, rather than just wireless interoperability.

Certainly in an Internet Protocol world, distinctions between voice, data and video disappear, but in the near term there are significant differences. It is also clear that thanks to public safety organizational leadership and support from the federal government, there is recognition of the wireless interoperability problem by elected officials, and there are highly effective programs to address wireless mobile interoperability (in which SAFECOM and NPSTC are the key leading organizations). Focus Group 1D strongly supports those initiatives, and describes in the box below how its work is complementary to those efforts from a more technical perspective.

There is one critical governmental difference. There is no similar national program to address the broader emergency response community and inter-organizational data communications interoperability problems and gaps on which Focus Group 1D's efforts have focused.

Comparing Current Public Safety Communications Initiatives and NRIC 1D

NRIC 1D believes its efforts are consistent and complementary with the emergency communications activities of SAFECOM, NPSTC, and their affiliates, as each of these organizations strive to enhance public safety interoperability. When viewed from a communication layer perspective, this becomes more apparent. There is general agreement that future infrastructure networks should be IP based, and that new multimedia and data services should be developed to work over IP. The current TIA standards for public safety interoperability, resulting from Project 25 (P25) and Project 34 (P34), all offer IP layer connectivity for their data services. The primary focus of these TIA standards has been on establishing common wireless air interfaces at the communication layers below IP, whereas the NRIC 1D activity is primarily focused on a common architectural framework above (and including) the IP layer in such areas as end-to-end security, policy, identity, and content management, as well as common methods of information exchange. These areas above the IP layer are critically important to interoperable PSAP-to-first responder communications.

With the current trend of responsibility for emergency services information technology and inter-organizational communications migrating to government IT organizations, there is an anticipated demand for more IT-centric architectures which can facilitate the unified operation of these networks. The NRIC 1D framework leverages IT-centric standards and any extensions to these standards necessary for mission critical operations.

The NRIC 1D Focus Group has proposed Voice over IP (VoIP) services extending out over broadband speed wireless interfaces, whereas the existing P25 voice services are optimized for narrowband wireless interfaces and do not require an IP bearer.

These alternative voice services can coexist, and two factors will determine whether and when the transition to wireless VoIP services will make sense for a given public safety agency: 1) the challenging economics of wireless broadband deployments compared to narrowband networks when trying to cover large geographies with high coverage reliability, and 2) the quality of service guarantees of VoIP in meeting the mission critical aspects of public safety voice communications. As VoIP technology improves, it is very likely that it can meet the latter requirement, but matching the coverage economics will be much more difficult. Regardless, the NRIC 1D architecture accommodates both alternatives seamlessly by including gateways that can interface P25 and VoIP services. This required internetworking may be simplified by possibly leveraging and extending upon the current P25 InterSubsystem Interface (ISSI) draft specification, which is VoIP-based.

5 Analysis, Findings and Recommendations

5.1 Comprehensive Interoperability – An overriding goal

5.1.1 Why Interoperability is Needed – the Value Proposition and Context

A critical weakness of current emergency communications systems is that agencies are isolated from each other. Wireline telephones do not help emergency responders in the field and do not allow the sharing of data among organizations.

Current methods to achieve mobile wireless interoperability include:

- Spectrum management to achieve some common channels between agencies
- Boxes that interconnect the landline side of radio networks to allow cross system communications with otherwise incompatible systems
- Standardization of the air interface and landline side of radio networks to achieve more interoperability (P25) [18]

Focus Group 1D recommends a much more far reaching notion of interoperability. We propose that all landline and all wireless networks support IP data services, that they all have common protocols and common security, and that they are all capable of running the same applications. Focus Group 1D proposes major national initiatives to address these needs, like the excellent and effective ones in the mobile wireless area.

By way of example, in a hazmat incident in a building, data sharing should be enabled among first responders of different agencies, and their agencies (where SAFECOM has focused). But it should not stop there. The following have data that may be useful to a hazmat response, or need these enriched data in real time:

- the building owner (e.g., building plans)
- the chemical industry (e.g., CHEMTREC's center describing the properties of various chemicals)
- public and private public warning systems
- 9-1-1 and homeland security agencies
- the area hospitals (e.g., casualty information on incoming patients)
- the mayor's office (e.g., situational awareness)
- the adjoining schools (e.g., shelter in place or evacuate)
- adjoining building owners (e.g., shelter in place or evacuate)
- the transportation agencies (e.g., best routes in for responders; best routes out for evacuation)

[18] In addition, a few other near-term initiatives are identified in SAFECOM Director Dr. David Boyd's recent congressional testimony. See http://commerce.senate.gov/pdf/boyd.pdf

- the local telephone company (e.g., with a major switching center in the adjoining building)

5.1.2 The Multiplicity of Organizations that Must be Linked

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 that will be linked by the future network. It is not intended to be a comprehensive list. Surely whole categories of participants have been overlooked. 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.

The future emergency services internetwork must include far more than only 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)[19]

[19] 180 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; more and more can provide pictures; in the near future we will have 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.

c. Business safety providers (e.g., telematics, alarm monitoring systems; hazmat service providers)
d. Hospitals. Clinics
e. Public health
f. Emergency management
g. Transportation
   - Departments
   - Different transportation modes (e.g., railroads, ports, trucking)
h. Non-governmental organizations: Red Cross, Salvation Army, CERT, mountain rescue groups, etc
i. Mental health organizations
j. National Guard
k. US DOD
l. Utilities, public works, recreation departments
m. Media
n. Schools
o. Critical infrastructure companies

This does not mean at all that every organization or agency connected to the internetwork should have all the same rights to send and receive communications. As is noted repeatedly in this report, technical capability is different than policy. Rights are policy decisions. The internetwork must have Facilitation Service tools to implement such policies. But those rights decisions must be made by the appropriate authorities, not by the network configuration or the tools themselves.

5.1.3 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 agency users. Indeed, in many instances, with appropriate protections, it might be shared with some non-emergency governmental users. This should 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.

It needs to be the same network for day-to-day incidents as for mass disasters and terrorist attacks.[20] 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.

It is inefficient and a detriment to interoperability to fund separate networks, (e.g., health alerting separate from emergency medical data sharing, or a terrorism alerting network separate from the regular 9-1-1 network, or a national warning system that is not a use of interconnected set of local and state networks used for all emergency purposes). All should use the same basic network. (Use rules, protocols and customer premises technology may, of course, vary by incident and agency type.)

5.1.4 Avoid Confusion in Discussion of the Interoperability Building Blocks

Making Appropriate Distinctions

It is critical that discussions of "Transport" issues be clearly separated from those about the "Data" that is transported, and from the "Applications" that manage the data. Similarly "Applications and Tools" used to act on data should be considered separately from the "Policies and Protocols" governing their use.

Many of Focus Group 1D's recommendations are on transport (i.e., the movement of multi-media) which 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, and on common services (e.g., facilitation services) so reference is made to the critical importance of those as well.

Focus Group 1D does not address, except in passing, two other key aspects of emergency communications – and these should not be confused with the discussion of transport, data sets and facilitation services. 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. They also include tools that might be shared by a number of agencies such as intelligent message brokers, common geographic information systems and the like. Policies and protocols are the "use rules." They determine which agencies and staff can send and

[20] Public safety organizations make similar distinctions using slightly different terms, such as "mutual aid" and "task force" incidents.

receive which kinds of data, when and how, and what is saved. They determine how emergency response may be conducted in this new data rich environment.

The transport, data standards and facilitation services recommendations made do not determine the answers in these other two categories of interoperability. Indeed, Focus Group 1D strongly believes 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, enabled by cooperative facilitation services, mean that vendors will be building for a national market, so that prices for emergency agencies should fall and / or 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. Focus Group 1D cautions that many entities seem to be working on isolated "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.

Policy and Rules Determine Use, not Architecture and Systems

Just because data can flow everywhere to every agency and staffer does not mean it 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 an overwhelming plethora of new information inputs (what students of the Bible might call a Tower of Babel). 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.

Focus Group 1D thinks 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 at a high level is the SAFECOM Program within the Department of Homeland Security. Focus Group 1D's proposals provide the choice of sharing information, which seldom exists today. They also call for the creation of institutions and processes to address the setting of information sharing policies. Focus Group 1D's proposals do not determine how and to what extent that sharing will occur.

Thoughts on an Enterprise Architecture Methodology for Emergency Communications

The term architecture framework (AF) may not be as commonly known as enterprise architecture (EA), yet both concepts are associated with the same structured process industry and government around the globe use to accomplish mission goals and save resources. While the concept of an enterprise architecture has its roots in the information technology (IT) world, it also fits the voice, data, and video applications of the public safety wireless communications world.

The Enterprise Architecture Interest Group (www.eaig.org) is quick to point out impressive EA implementation successes by such companies as Volkswagen of America, Disney, Best Buy, GM and Swissmobile. At the same time, the United States General Accountability Office (GAO) has, for over a decade, promoted the creation of EAs through the use of AFs. The GAO recognizes that AFs can clarify and help optimize the interdependencies and relationships between business operations, the underlying infrastructure, and the supporting applications across a large federated organization. The United States Office of Management and Budget (OMB), Federal Enterprise Architecture Program Management Office, Federal Departments and Agencies have concurred with this assessment and are actively undertaking EA planning and implementation efforts. It is only logical that the emergency response communities apply the same structured approach that utilizes a common methodology provided by an AF to produce an architecture framework for emergency agencies and organizations for defining and resolving large-scale interoperability challenges.

The architecture framework outlines "what" the overall structured approach is for facilitating interoperability and, through the details of this structure, indicates "how" the architecture (and its components) will operate through the development of interface standards. In short, the architecture framework provides rules and guidance for developing and presenting architecture descriptions.

Emergency response requirements are often developed, validated, and approved as stand-alone solutions, for specific domains within the broader emergency enterprise to counter specific scenarios. This approach fosters an environment in which specific safety agencies make acquisition decisions which, in an inter-disciplinary/inter-jurisdictional context, are not fully informed by, or coordinated with, other safety components. Proposed systems struggle through a budget process and acquisition pipeline of specific domains/professions that are inefficient, time consuming, and do not inherently support interoperability. Piecemeal, stovepipe procurements of new and legacy systems result in a less than optimal performance.

To address the challenges of the twenty-first century, the architecture framework concept (or enterprise architecture methodology) promotes a capability-based construct that facilitates planning in an uncertain environment by identifying a broad set of capabilities as participating elements in an overarching system of systems. To accomplish this transition, the enterprise must first be defined to include all organizations in emergency response, institutions and/or processes that can represent that diversity must be set up, and then a decision process that performs the following tasks must be implemented:

1. Assess legacy and proposed systems in the aggregate
2. Define desired inter-disciplinary/inter-jurisdictional capabilities
3. Derive and validate mission area requirements
4. Consider the full range of solutions, and decide.

To achieve substantive improvements in inter-disciplinary/inter-jurisdictional safety operations and interoperability in the future, coordination among safety components is essential. The decision process must be reformed to employ a synchronized, collaborative, and integrated systems engineering approach that better facilitates capability-based planning.

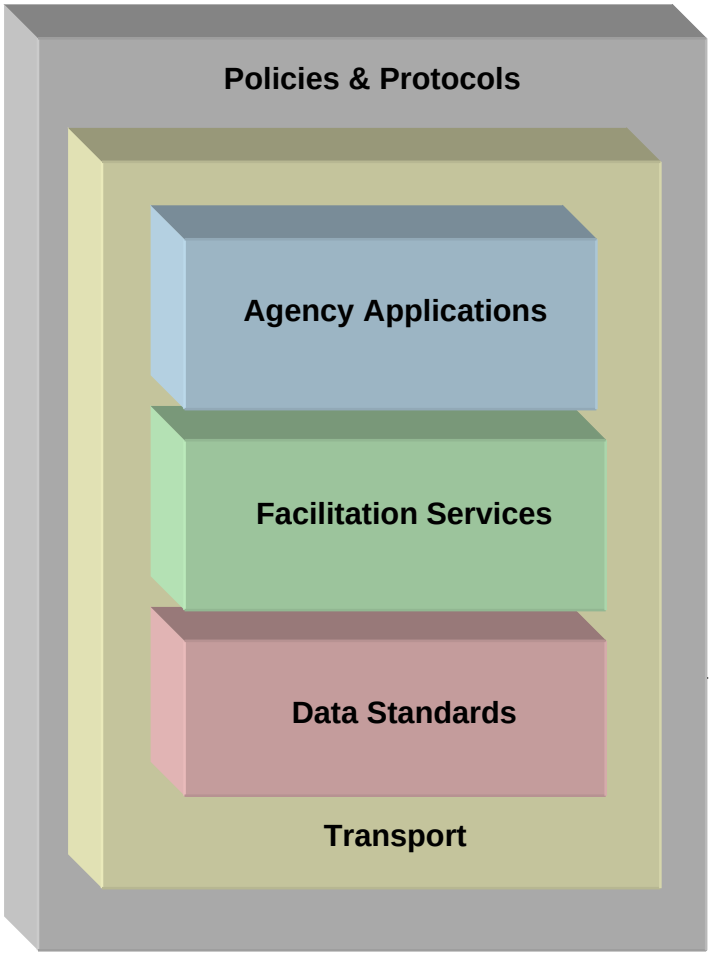
Furthermore, as emergency response enters an era of network-centered, multi-discipline, multi-jurisdictional operations, the ability to portray and understand complex many-to-many relationships becomes even more important. Capabilities must be able to "plug-and-play" in an inter-disciplinary/inter-jurisdictional, nationwide, multimedia environment.

To achieve this ability, there must be a mechanism for incorporating information technology (IT) consistently, controlling the configuration of technical parts, ensuring compliance with technical "building codes," and ensuring efficient processes. Architectures provide this mechanism by serving as a means for understanding and managing complexity.

There is no such effort focused on linking the overall emergency response enterprise, which is composed primarily of state, local and private organizations. There are organizations performing this function for radio communications for traditional public safety; no similar structures exist for the broader safety enterprise definition used here and the broader forms of communication described in this report. Addressing this gap is a critical national policy need.

5.2 Components of Interoperability

There are several building blocks that must be addressed and then put into place to achieve effective data interoperability in a state or region, or nationally. Some of these are shared resources, while others are components that will be unique to individual agencies (See Diagram 4 below). The needed blocks that must each be addressed are data *transport*, common emergency response data *standards*, *facilitation services* shared by all emergency agencies, individual (or shared by some) agency *applications*, and the *policies and protocols* that govern the use of the system when data interoperability is achieved.



Policies & Protocols

- Multi-level governance
- Distribution and response protocols
- Policies for Facilitation Service tools

Agency Applications

- Software to support agency/community operations
- Tools to manage data, enhance data and support decision making
- Network services

Facilitation Services

- Shared utilities available to all authorized agencies, such as Authentication, Rights Mgmt, Routing Directory, and Diagnostic services

Data Standards

- Standard message structures and datasets so information can be universally understood
- Legacy systems build interfaces to standardized "center"

Transport

- Connect all agencies and organizations
- Physical connections (wired and wireless)
- Management of data delivery between network devices

Diagram 4: Emergency Communications Interoperability Layers

An overall emergency communications technical, policy and governance framework is required that identifies all the elements of the Emergency Services internetwork and associated functions. This framework encompasses the multitude of standards,

technologies, interfaces and facilitation services, as well as the common principles and guidelines for interconnecting all the different networks. As previously noted, emergency communications should be viewed as an overall "enterprise" without a single owner. Such an enterprise cannot exist unless the stakeholders support it. Therefore a fundamental transition issue is to have all the stakeholders aware of the advantages and efficiencies of the approaches discussed herein. A major outreach and education effort needs to be undertaken.[21]

The following discussion is divided into a number of major sections: transport, data standards, facilitation services, agency applications, and rules / policy. Within each of these sections, the specific recommendations from the Focus Group are summarized, and the transitional issues that need to be addressed in order to achieve them are discussed.

5.2.1 Network/Transport

New emergency networks and applications using them must operate in an open architecture, using internationally standardized protocols, open API's and standardized datasets. Interoperability of equipment elements of a network 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, including wireline and wireless. There needs to be an expedited movement toward IP packet-switched communications networks, supporting mobile and fixed voice and data services.

Focus Group 1D proposes that the transport layer be quite explicitly separated from content, customer applications, use rules, policies and protocols – both for discussion purposes and architecturally. In the long term, common transport, common protocols and a wider variety of applications that can run over any transport to any device are required. Focus Group 1D advocates common authorization mechanisms so that policy, which in general should be local or profession-based (e.g., a public health vertical), can be uniformly enforced throughout the system regardless of transport.

5.2.2 Embrace Diversity through an Emergency Services Internetwork – a Series of Interconnected Networks

Emergency response systems are diverse. There are approximately one hundred twenty thousand emergency or emergency support agencies.[22] Even if there were the

[21] Please see Policy Issues, Section 5.6.
[22] Focus Group 1D again notes that our definition of emergency response agencies and emergency services is much broader than the traditional term "public safety."

funds to pay for it and all these agencies were willing to let some other entity run the network (neither of which is true), a single national emergency network is the wrong answer. NRIC Focus Group 1D recommends the future Emergency Services internetwork be a network of networks, a set of tools, interfaces and policies needed to connect a series of separate physical and virtual networks. Just as emergency agencies should be able to select their own applications, collections of them should be able to create their own networks. Those in turn should be connected to the Emergency Services internetwork.

The unifying task therefore is not to build any networks, but to work on their intersections, to develop the standards and common tools that make them work together.

It seems clear from recent events that the notion of who must communicate in disasters is much more expansive than previously considered. School bus drivers, commercial haulers, and utilities need to be able to communicate with public safety organizations seamlessly. If the communications networks of these diverse users were IP based, some commonality of protocols and security with them was achieved, and IP connections between their networks and the public safety IP networks were pre-engineered, a level of capability that can now only be dreamed about could be achieved.

Fortunately, by standardizing on all IP based systems, achieving this redundancy is easier. Most facilities are in range of a variety of different access networks (e.g., terrestrial and satellite). In most cases, they can relatively easily subscribe to redundant broadband connections to points of presence for a variety of networks. In the short term, the emergency response community can generally and relatively easily access the various commercial networks; every emergency agency needs broadband access, and most, even in rural areas, are within simple reach of it at reasonable cost. There are a number of IP networks: public, schools, state fiber, local government fiber, satellite, and commercial Wi-Fi networks. Government owned networks, virtual private networks, and other IP links will gradually be added to the commercial networks to achieve the levels of redundancy and diversity that are needed. Private networks can be used on a daily basis; public networks can serve as additional resources to the emergency community, when needed.[23]

Indeed, if the transport mechanisms are always IP-based, or could carry IP, then all the facilities in a single installation can share access networks, which simplifies the situation most commonly found today where every subsystem has its own, separate access facility.

[23] In some instances, emergency communications might have requirements which might preclude the use of these commercial networks.

Multipurpose, All Hazards Emergency Services Internetwork

Focus Group 1D believes this internetwork will, like the Internet, provide robustness and redundancy. Indeed, it is important to recognize that access technologies are evolving faster than other technologies. Focus Group 1D envisions that each municipality, agency, region, state or tribe will have a variety of physical networks, some wired and some wireless. Each of these networks will 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 be sent over an IP based network. 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 for 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. There should be a transition away from special purpose emergency networks.

Focus Group 1D proposes that homeland security agencies send and receive appropriate data by interconnecting to the "Network of Networks" described here. A separate network or set of applications for either homeland security or for disasters is not advocated; communications systems used every day have a better chance of working when disasters strike. It should be possible for each network to use both public and private networks for transport. Focus Group 1D recommends 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. Devices should be able to seamlessly switch between networks, rather than requiring people to carry multiple devices. By standardizing on IP transport, the costs of such systems should be modest; only the physical transport layer needs to be able to access multiple networks.

5.2.3 Wireless versus Wireline

The internetwork will encompass all communications transport forms. Subject to timing driven by the transition concerns and quality of service principles, the physical, organizational and policy separations between wireless and wireline communications need to be abolished. Similar distinctions between voice, data and video (and on-scene versus inter-agency 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. 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 that continue to support these distinctions are reinforcing counterproductive silos.

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.[24] Focus Group 1D further recognizes 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.

Significantly more spectrum, in large contiguous chunks, is required so emergency response agencies can use IP efficiently. The narrow band spectrum that will be provided to emergency agencies when the digital television transition is completed will certainly be of significant help in meeting safety needs, particularly for interoperability. It will not, however, be sufficient to meet wireless broadband needs.

5.2.4 IP Transport and Web Services

Focus Group 1D recommends that IP should be used and sees no reason not to adopt this commercial standard, nor is there an obvious alternative.

Focus Group 1D believes web services are the appropriate approach for most data interoperability. IP particularly lends itself to the diverse communities and diverse databases involved here and discussed in Appendix A. In addition to the facilitation service agency registries discussed below in Section 5.4.2, cached sets of authoritative data are needed, as are a web services Uniform Discovery and Data Integration (UDDI) of them. By representing data uniformly in XML form, a reasonable way to format it for display can be provided 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 expiration 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 data. 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 Redundancy and Reliability

There is a common perception that today’s emergency networks are both redundant and reliable. While that is certainly true in some cases, there is much to be desired as America learned during the recent hurricanes. The best results found today are in

[24] In this regard Focus Group 1D notes the importance of the work of 3GPP2 on header compression standards.

mission critical public safety radio systems. The best practices for constructing reliable systems should be adopted across the country in all emergency communications systems.

5.2.6 Redundant Connections to the Networks

Network connections become more important as media types (e.g., voice, data, and 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.
Best practices, if not policy, include redundant physically divergent broadband connections using more than one system/carrier, and having access to more than one point of presence (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.

5.2.7 Use of Radio Spectrum

For years, public safety has wrestled with spectrum and technology issues that prevent individual agencies from having sufficient communications capability to perform their missions, much less to interconnect with other agencies when mutual aid is involved. As was 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, emergency agencies 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 (i.e., 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 tens of thousands of emergency agencies, having probably about as many licenses, is that their spectrum is scattered across multiple bands, none of which has enough bandwidth to handle the more demanding amounts 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.

Emergency agencies need a dramatic increase in the contiguous 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, Focus Group 1D believes 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 mobile interoperability: the multiple discrete bands now assigned to local/state public safety agencies by the FCC.[25] The point here is that spectrum allocation needs to be rethought based on emergency agencies' need for high bandwidth data sharing in addition to voice communications, while simultaneously and effectively addressing interoperability.

5.2.8 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. Focus Group 1D believes 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. Focus Group 1D specifically recommends against relying 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

[25] In July, 2004, the FCC adopted a plan to resolve the problem of interference to public safety radio systems operating in the 800 MHz band by approving a new band plan that separates generally incompatible technologies (used for public safety and commercial purposes, respectively) with the costs of relocating 800 MHz incumbents to be paid by Nextel (now Sprint Nextel).

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.

5.2.9 Transport Transition Issues

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 communication of some modest levels of emergency data (e.g., incident alerts) among almost all emergency agencies today. This is just a first step and the ultimate answer will involve other public and private IP networks to meet the particularly high requirements of mission critical voice, video and other similar communications uses. It will also involve the development of sophisticated tools and policies to govern actual information sharing (one agency's access to the data of another). These latter issues are very difficult; getting started with emergency data messaging is not -- if it is given serious focus by national and profession leaders.

Focus Group 1D foresees a mix of commercial and government owned networks. Indeed many smaller agencies are already deploying commercial IP systems because they cannot afford to install government-owned networks with equivalent functionality and they have determined that the usefulness of the commercial systems outweigh the concerns they have about reliability and security. Indeed, the Internet model predicts, quite accurately, that using multiple connections with common protocols yield very reliable systems, and security is best implemented at higher layers to afford seamless security from end to end. If we start by using the Internet for data sharing, and gradually add to the Internet connectivity with more managed, controlled IP connections services and improved reliability will seamlessly expand.

The Focus Group 1D recommendations do not either assume or require immediately replacing most of the current safety IT/communications infrastructures – or require a "fork lift" upgrade, or a flash cut transition to them, rather than a gradual phasing in. Indeed, the use of IP allows a far smoother transition to the future than past experience. Physical interfaces and policy rules are the key elements. For example, some or most computer-aided dispatch systems in use today could accept (push or pull) or send data with external sources if an interface were built to the new XML data standards. What Focus Group 1D advocates is adoption of more common protocols, applications and security mechanisms to provide seamless end to end connectivity, across all agencies and across all networks.

The nature of this broad and diverse emergency response infrastructure means that adoption and change will come incrementally. Interagency wired, satellite-based and

other IP transport systems will make it easier for rural agencies to close the divide with their urban counterparts. With a broadband connection, rural agencies can access exactly the same technologies (particularly if shared systems are developed). This is just one more reason why the focus of the Federal Communications Commission and Congress on rural broadband deployment is important.

System designers 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. Given the dynamic and unpredictable nature of emergencies, it is imperative that the emergency responder agencies possess robust and flexible communications capabilities.

5.3 Current and Future Data Sources; the Need for Standards

5.3.1 The Explosion in Data Sources

In Appendix A, Focus Group 1D describes many of the types of data that will become available to response agencies. This is not intended to be a comprehensive list, but is intended to describe the diversity of data types. There is also an extensive list in the SAFECOM Statement of Requirements. The critical point is that there is a great deal of data available in electronic form, but most of this data is not now available at all (or at least efficiently) to every affected response agency. The internetwork must be able to handle large amounts of voice, data and video. The issue Focus Group 1D addressed is not 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. Policy and protocols, not network architecture, will depend on the content of the data.

Additional information and transport media will better prepare emergency response agencies to provide and coordinate resources in answering calls from the public. The networks proposed are “all-hazard” and “all emergency.” They are therefore agnostic as to which data travel over them; instead, the form of data is more important: real time or not, for example.

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 emergency agencies. 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

- These 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.

Methods must be developed for identifying the availability of new data sources, providing leadership to develop standards for them so that they may be accessed,[26] and providing registration mechanisms so that their availability can be advertised where permissible by law or public policy.[27] Emergency agencies must be equipped 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.

Other issues which arise from new sources of data include: how is the new data logged? Which media streams are recorded and which are not? Who can access them after an emergency and for what purpose?[28] The answers could have profound implications for users. This is another good example of the need for new policy and protocol discussions that extend beyond traditional boundaries. These must include leaders from all of the affected professions and organizations.

5.3.2 Categories of Emergency Data

There are several different categories of emergency data. Some of these include:

- Call data - data relative to a specific 9-1-1 call
- Location data - data related to a location that does not change from call to call, or incident to incident
- People data - data related to the person calling or affected by the emergency
- Incident data - data created during an incident that is shared among entities responding to the incident
- Service data - data related to the entities responding to the incident. Service area boundaries would be an example
- Resource data – data about the staff and things involved in response
- Response education data – data which assists agencies in responding properly, such as procedures, protocols, or training

[26] This is a particular challenge as the development of data useful to emergency response agencies is very often 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.

[27] 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.

[28] HIPPA contains a complete exemption for the sharing of medical data with responders during an emergency (and for treatment). The exemption does not apply to subsequent access to that information for non-treatment purposes.

- Data from decision support tools

Each of these data is separate and distinct, and probably will be stored and managed differently. None of them should be in any way tied to (i.e., determined by) the underlying network. Focus Group 1D does 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 described, related 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 databases 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 URL. Service and Resource data is located at the service provider (e.g., PSAP, Police, fire, poison control, and transportation). Incident and resource data are 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 by public health and homeland security agencies[29]) may be located anywhere.[30]

Focus Group 1D advocates a uniform security model that would control who has access and update privileges to such data (see Section 5.4.4 below).

5.3.3 The Value of Standards

Fixed and mobile system interoperability requires standards, including standardized message structures and data elements. 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

[29] Syndromic surveillance is the extraction of indicators of disease or bio-terrorism from a multiplicity of sources such as hospital admissions reports, 911 calls, EMS reports, pharmacy sales and the like.

[30] 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.

behind" rather than in a "revolutionary" or un-even 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[31]

Standards serve a variety of positive purposes. Economically, they improve quality and reduce acquisition costs by creating a large national and international market. The larger R&D resulting from creating for a larger market increases customer choice of components. The current system is characterized by a large number of proprietary data information systems, and a great deal of "one-off" information technology. Even where there have been efforts made to standardize data exchange formats, interfaces, and access protocols, these have generally been confined to professional areas (e.g., separate efforts for EMS, criminal justice, transportation, 9-1-1). This is a serious problem when the emerging demand for access to networks and systems is both among jurisdictions and between professions, not just within one profession in a single jurisdiction. It is only very recently that there have been standards conversations across emergency domains, but there is no aggregate data standards coordination effort, let alone one to produce common standards for all emergency response agencies.[32]

5.3.3.1 Standardizing Data Sets, Protocols and Interfaces: Current Activities

There is a general consensus among emergency response leaders, which Focus Group 1D supports, that data should be in XML. There is also an emerging consensus among them that standardized schema and data elements across all emergency professions are needed. While each profession may have terms which are unique to it, or unique understandings of certain terms, all can and should strive to have a common emergency language, starting with the message structures that are used and terms that are shared (i.e., time, latitude and longitude, sender, type of message, etc.). Such an initial effort is required to meet Focus Group 1D's recommendation of rapidly developing a limited set of common standard message sets.

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

[32] As noted in a number of other places in this paper, Focus Group 1D compliments and encourages emergency standards efforts in various areas. For example, the Focus Group strongly supports 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. The National Information Exchange Model initiative has the comprehensiveness this report recommends as a goal. The DHS Disaster Management Initiative-sponsored Emergency Data Exchange Language (EDXL) project has a diversity of agency leaders developing common emergency messages.

Wherever possible, open standards should be specified and used. 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 a way that allows networking between different equipment. Data should be self describing (e.g., XML with schemas and imbedded formatting).

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 until very recently. 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. There has not been a government leadership body with the authority to encourage, facilitate or order participation by all the relevant professions.

Some of the emergency response standards efforts occurring now include:

- Intelligent transportation (IEEE 1512 and ITE)
- Law enforcement community (Law Enforcement Information Technology Standards Council—LEITSC
- DHS Disaster Management, Emergency Interoperability Consortium, and OASIS (EDXL, emergency response generally)
- Justice community (the Global Justice XML Data Model, GJXDM)
- Project 25 Digital Radio Standards (APCO / NASTD / Federal agencies)
- XML.gov
- TIA (ANSI)
- DHS and DOJ (National Information Exchange Model, NIEM)
- NHTSA / NAEMSP / NASEMSD (NEMSIS)
- Hospitals (HL7 and Electronic Health Record initiative)
- Public health (PHIN)
- ATIS and NENA (9-1-1)
- OGC (GIS)
- APCO (CAD to CAD), and
- COMCARE (EDXL, vehicular emergencies and EPAD).

There are probably others. In addition, there are a number of national and international industry standards and standards efforts which can be used by emergency response, rather than reinventing wheels. All of the above, with the exception of NIEM and EDXL are sector ("domain") specific, rather than including all emergency agencies.

Another challenge is that it cannot take years to follow the traditional route to standards creation. A model of rapid development, rapid prototyping, deployment, real world use, and then improvement is needed.

5.3.3.2 Selecting Standards

A selection process to choose those standards that will be deployed in this ubiquitous IP internetwork is needed. Where the standards are fundamentally about safety, requirements need to be developed by all involved professions.

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 safety should be nationalized. On the contrary, by implementing national transport and data standards, and creating similar interoperability enabling tools, local and state choice and flexibility in information use, response protocols and the like can be increased. But there needs to be a national consensus of the key stakeholder groups on a number of key items discussed below.

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.

While each profession may have terms which are unique to it, or unique understandings of certain terms, Focus Group 1D proposes to have a common emergency language, starting with the terms that are shared (e.g., time, latitude and longitude, sender, type of message, etc.) and a set of common standard message sets to promote information sharing.

Selection of particular standards by a coalition of emergency response stakeholders is essential to achieve wide interoperability. In the longer term, and where standards do not exist, Focus Group 1D recommends development designated by coordinating bodies with a particular emphasis on standards developed by ecumenical processes including all relevant emergency response agencies. Unlike the traditional public safety agencies, which have entities like SAFECOM and NPSTC to focus on wireless issues, there is no aggregate emergency standards coordination effort in the emergency services and response domain, let alone one to facilitate the production of common standards for all emergency response agencies.

The recently initiated National Information Exchange Model (NIEM) is a step to resolve the dictionary part of this issue with a mission "To assist in developing a unified strategy, partnerships, and technical implementations for national information

sharing…"[33] The eGov Initiative of the DHS Disaster Management EDXL program to facilitate (through a representative Standards Working Group of emergency response agency practitioners) the development of specific emergency message standards that are common across the emergency communities also needs to be supported.

5.3.2.3 An Accelerated Standards Program is Needed

Focus Group 1D recommends a comprehensive and intensive, emergency response standards development effort, led by emergency response leaders with the resources to succeed in the project. The FCC should work closely with the executive branch of the Federal government to support the NIEM and EDXL public/private efforts to undertake this. There must be a single process where emergency data standards for information that must be shared between emergency professions are coordinated, if not 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. The process needs to be democratized, and that means providing financial resources to directly support involvement of national organizations representing emergency responders in standards and protocol development activities.

Focus Group 1D opposes the federal government setting standards itself, except as a very last resort. It similarly opposes re-inventing any wheels.[34] A comprehensive, and intensive, emergency response standards effort is needed, led by emergency response leaders with the resources to do it right and quickly. Focus Group 1D proposes that the FCC work closely with the executive branch of the federal government to fund a public/private effort to:

- Establish a coordinating committee with representation from all stakeholder groups[35]
- Create a shared website, and tools to search and share the results of each project, and shared projects
- Identify emergency response requirements
- Reach consensus on a limited number of shared emergency messages[36]

---

[33] http://niem.gov/

[34] The leading example of effective involvement of local, state and federal leaders in a cooperative standards development process is the Global Justice initiative. This effort of all the parties in the Justice community (law enforcement, courts, probation, prisons, etc.) has produced a common dictionary of terms and a data model. EDXL and other initiatives are reusing its content.

[35] The Focus Group supports the new pilot National Information Exchange Model (NIEM) initiative by DHS and DOJ, the goal of which is to develop a national focal point and process for common standards development. The Group encourages its funding, and the inclusion of all emergency professions in its governance.

- Determine what is available already from the private sector and prior emergency response standards efforts
- Map the overlaps and identify the holes
- Facilitate rapid action to address those[37]

5.3.3.4 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 open architectures and standards use by their vendors and grantees. Significant federal grants are being made today without such requirements. Focus Group 1D recommends this be changed immediately to a system where grantees and vendors are required to adopt those emergency standards that are currently available (as designated by the federal granting agency), and to incorporate new standard data sets as they are issued. For now this would include:

- Interoperable and seamless service using open architecture, IP, XML, web services, VoIP (where appropriate), SIP
- Best efforts to incorporate existing standards and common vocabulary: Global Justice XML dictionary; EDXL; OGC, NEMSIS, CAP, VEDS, etc.
- Other commercial standards of general applicability designated by the granting agency (ideally coordinated by DHS)
- In the future: new standards designated by coordinating bodies such as NIEM and EDXL -- with a particular emphasis on standards developed by ecumenical processes including all relevant emergency response agencies[38]

5.3.4 System Standards: 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

---

[36] The very successful development, approval and deployment of the OASIS Common Alerting Protocol is a recent example. One data standard that will help guide all emergency message sets is a standard XML "emergency message Distribution Element" to be used by all emergency messages for routing purposes. This is now in the formal standards consideration process of OASIS, along with a set of proposed Resource messages. These latter two have been produced in the EDXL process. See footnote 38.

[37] The Focus Group strongly supports the EDXL emergency data standards facilitation that is seeking to accomplish exactly these goals, including establishing on-going communications between the standards efforts of the various emergency professional organizations. All emergency organizations have been invited to participate in developing a set of shared message structures, using the content of other standards processes, such as the Global Justice initiative. The project is sponsored by DHS, involves leaders of most national emergency response organizations, works with private sector groups led by the EIC, and is staffed by COMCARE and others.

[38] Focus Group 1D believes NIEM can become this with the proper support and leadership.

session (i.e., 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.

5.4 Facilitation Services

Facilitation Services is a new concept, deserving of significant collective attention by the affected federal agencies and by the emergency response community. For data to be broadly shared, every network and/or application cannot have its own rights management section, its own routing directory, its own security and authentication systems, and so on.[39] Instead, the emergency response communities need to develop and manage a set of shared "Facilitation Services": authentication, rights management, routing directory, security, network coordination and perhaps others.

This is an area that needs focus from the emergency professions, and federal facilitation and financial support. If commonality of networks, protocols and security mechanisms is to be achieved, some underlying shared facilitation services that achieve this commonality need to be put in place. The architecture advocated does not generally rely on "one" technical version of anything. Rather, Focus Group 1D sees interconnected and federated subsystems arising (i.e., not a "single box"). However, there must be agreement on what mechanisms need to be deployed, how they will be interconnected, how federation will be achieved, how they will be funded, and how governance will be handled.

5.4.1 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 which agencies) 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 becomes out-of-date, inaccurate and incomplete. The network should make it easy to publish data. Data should be

[39] The need for facilitation services is just as great at the local and regional levels, as it is at state and national levels. In addition to avoiding duplication, multiple sign-ons, and inaccuracy, they can provide the central focal point for efficient, integrated policy making and implementation on data rights and flows (as opposed to each agency or town within such areas doing its own.)

published in small parts that are aggregated by the network, rather than coalesced into very large, centrally controlled data warehouses.

Agencies should be able to decide what data they want, for what geographic 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.

5.4.2 Unified Registration Systems

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 public and 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 available. These registries must be available to all agencies, as it is impossible to predict who will need the data when emergencies occur. Web services are a very useful technology in this regard.

5.4.2.1 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, 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 addresses. Only authenticated and authorized users would have access to it on a non-discriminatory basis.[40]

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

[40] Funded in part by a grant from the Department of Justice, COMCARE has deployed a prototype of such a facilitation service directory, called the Emergency Provider Access Directory (EPAD), and designed a production version. It is working with over 15 national emergency organizational partners in the NEARS project to develop and deploy it. This a good example of both a specific Facilitation Service and the shared, non-profit ownership process described here.

the appropriate levels of government. Focus Group 1D suggests 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 noted, there are many sources of data and facilities that are not normally thought of as emergency services 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 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. No single emergency response agency has the resources to field such a national directory of agencies on its own. In order to minimize this resource barrier to deployment, and improve accuracy, this function should be done as a shared utility. 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 all forms of devices.

These directory tools need to be built and tested. Routing directory, rights management, and similar facilitation services need to be established along with business operations rules. Focus Group 1D recommends a rapid, but incremental deployment.

Individuals and agencies may not be able to predict data they require for an incident. As a migration strategy, regional network providers can subscribe to as many data sources as possible on behalf of their subscribers. These network providers can make those data sources available to their users, either as a push or a pull, based on existing or modified data relationships. Recognizing that not all networks are created equal, special provisions can be made by each network provider to take advantage of the capabilities embedded in their network to approach the desired network architecture.

Transitional Task
Scalability is a significant issue. Focus Group 1D recommends model state and regional deployments of a full set of Facilitation Services to gain lessons, particularly about scalability, before broader deployment.

Long Term
In the longer term, business operations rules that govern the various services and transactions are needed. These rules need to be flexible to accommodate the different configurations that state and local agencies may have. In addition, agreements must be in place to ensure that the agencies will maintain updated and accurate information.

5.4.2.2 Information Discovery Services

Information Discovery Services must be available that allow entities in the Emergency Services internetwork to find easily relevant data and information sources. The discovery process enables nodes in the Emergency Services internetwork to find crucial resources without prior knowledge of their existence. The registries must advertise availability, nature, extent and applicability of the various data sources as well as the access mechanisms for them. The creation and availability of such registries will allow the emergency response agencies, access to vital and relevant information. These should be managed by appropriate groupings of emergency agencies.

Transitional Task
While an automated approach using web services is the future vision, a reward system could be put in place to encourage potential publishers of data to make their available data known in specific emergency directories. Advertising the availability of data could be accomplished on a secure web site with tax incentives provided to those publishers that participate. Individuals, agencies or participating network providers would be granted access to the data availability listings based on their authorizations.

Creation of these services will prevent duplication of efforts, and will promote reuse of existing implementations and efforts. Therefore, efforts must be initiated, almost immediately, to enable the creation of these services.

5.4.2.3 Flexible Addressing

All parties and systems associated with the internetwork should assume that all emergency response devices (e.g., a radio or laptop computer) will need to be available on the public Internet, even though most will be connected through private networks. When disasters strike, assumptions on infrastructure tend to fall apart as Hurricane Katrina clearly showed. Flexibility is needed to respond. Systems needing well known addresses should rely on the Domain Name System (DNS);[41] dynamic DNS[42] may be appropriate for many systems rather than on static address assignments. Focus Group 1D advocates that public safety not deploy Network Address Translation devices (NATs),[43] especially when IPv6 is used. On the other hand, systems are advised to assume NATs exist and deal with the discontinuities they introduce.

[41] 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.
[42] 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.
[43] 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.

The use of IPv6 is recommended. While DoD has issued regulations mandating support of IPv6, there is currently limited support for it in commercial equipment. Given expected lifetimes of emergency communications 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 safety organizations. Focus Group 1D advocates that all safety systems should be using IPv6, but should be fully backwards compatible with IPv4 systems.

5.4.3 Security

The goal Focus Group 1D seeks is to allow any (authorized) public safety agent to communicate: voice, video, text and data, with any other agent when they need to, securely. To do so implies a level of commonality of security mechanisms not available, and not contemplated, by any other effort of which Focus Group 1D is aware.

Where great strides have been made recently in data commonality and message commonality, and IP based protocol mechanisms are (slowly) converging within the safety communities, there is no effort this group knows of to select and deploy common security mechanisms across all networks and applications.

The fundamental problem is that there is no forum to work on this issue, and thus there is an urgent need to bring together stakeholders to select standards for authentication, authorization, integrity protection and privacy that can be ubiquitously deployed on all applications. Once such standards are selected, Focus Group 1D foresees a need to rigorously require they be used in preference to application specific standards.

There is also a need to educate local and state agencies about common policy mechanisms so that they may appropriately fashion policies that will meet their needs both in day-to-day and disaster circumstances.

5.4.3.1 Integrity Protection and Privacy

Data integrity should always be protected against modification. Privacy (i.e., encryption) of data will be required, with end-end authentication.

Once un-encrypted data has been released outside of closed networks into public networks it should be considered public domain. While all efforts should be made to protect sensitive data from inappropriate use, it must be recognized that the release of data from the publisher to the subscriber then becomes the responsibility of the subscriber to protect that data from misuse.

Access to network and information resources (e.g., security) should be governed by cryptograph-ensured access control, not separate physical networks. Instead, today each application deploys its own mechanism, and there are a plethora of ill conceived,

and unlikely-to-be-successful attempts at creating what are called "walled gardens,"[44] (i.e., special purpose networks where access to the network is so tightly controlled that security within the network can be assured). Focus Group 1D rejects the premise of such systems, and calls instead for security mechanisms to be applied uniformly at higher layers, supplanted by what is called "channel security" where needed on specific access networks.

Interconnection between emergency response networks and public networks provides much additional capability but raises some security concerns, especially when it is also necessary to connect state and local agencies to highly secure federal networks. Where these networks need to interconnect to federal or other networks that are walled gardens, carefully managed applications gateways must be deployed at the edge of the walled garden networks that can allow secure communications of permitted data from such networks across state and local networks even when those networks are also interconnected with public networks.

In the past, it has seemed easier to physically restrict users on special purpose public safety communications networks (i.e., create a walled garden). Focus Group 1D believes it is no longer appropriate to do so, and thus advocates that "walled garden" networks be discontinued, and rather that uniform, cryptographically based authentication, authorization, integrity protection and privacy controls be applied to all networks over which emergency communications must happen. Focus Group 1D specifically believes that the "network" should not be "trusted." Rather, every communication should be considered to be transiting insecure networks, and thus needing cryptographically based security. Public safety agencies should take reasonable precautions to assure that their networks cannot be used by unauthorized persons, but it should not be assumed that such precautions will be enough.

The focus should be on deploying appropriate security mechanisms on top of the basic packet transport infrastructure to provide the security needed. Because Focus Group 1D advocates a mix of public and private IP transport networks, it will be necessary for the security discussed here to run at the session layer. Security should be uniform. It should always be enabled, on every transport, for every communication.

The security mechanisms Focus Group 1D recommends include:

1. Authentication, as discussed above, which should identify users and not devices, in a federated security system

[44] 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.

2. Integrity protection. In all cases, data integrity should be protected against modification
3. Privacy. In most cases, privacy (i.e., encryption) of data will be required

5.4.4 Rights Management

Linking networks will require a system(s) that will assure that only authorized parties may participate, but there also must be 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. Focus Group 1D recommends the development of public and private institutions for this purpose, and the development of tools to enforce the rules. (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 that handles agencies' addresses.[45]

There are two distinct areas of rights management: identity rights management (i.e., authorization and authentication of agencies, roles and/or individuals), and data rights management (i.e., rules affecting use of specific data). Focus Group 1D has noted the difference between application level access controls and data based access controls. The former controls what operations a user may perform, without regard to specific data items. The later attaches controls to a specific datum (or class of data), and specifies controls on that datum without regard to the operations performed. Both mechanisms will be needed to meet varying needs. Both mechanisms must share role definitions and policy publishing facilities so that interoperability can be achieved.

5.4.4.1 Identity Rights Management: Control Authorizations; Flexible Rule Sets

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.

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. Incident commanders and dispatchers must be allowed to adjust authorizations to fit on-the-ground conditions. While it might be useful to

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

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.

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 the institutions to accomplish this for the overall emergency enterprise discussed above are lacking. In order to minimize this resource barrier to deployment, and improve accuracy, these need to be done as shared utilities. Many emergency response agencies do not have the resources to field such systems on their own, much less keep them accurate. For fully effective use, state laws that address information sharing and privacy will have to be harmonized, and the resources to implement these systems will need to be provided.

5.4.4.2 Agency/Role/Person Authentication

There must be a trusted way, a federated approach, to credential agencies, roles and individuals, to provide them with appropriate authorizations, and to allow them access to and use of the network.

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 (e.g., 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.

Some access networks are inherently more susceptible to security concerns (e.g., radio networks) and may need device authentication for the access network in addition to person authentication for the application. Systems designs should separate these issues with the goal of achieving the effect of “single sign-on” to all applications via any device. Generally, device authentication to an access network can be invisible to the user of the device. Focus Group 1D cautions the systems designers who are specifying device authentication to consider the impact of such mechanisms in disasters, where out-of-area responders may need to be admitted to an incident network. Policy and admittance decisions should primarily be made at the application level, with minimal effort needed at the access network / device level to achieve interoperability.

Structures are needed for credential provisioning and dissemination, and to formulate the policies and procedures for governance and operations.

Achieving ubiquitous authentication will take some time, and application specific authentication systems will be deployed for some time. Systems designers must plan for how transitions will be managed so as to maintain adequate security without degrading the ability of responders to do their jobs.

5.4.4.3 The Rights Management Facilitation Service

The Emergency Services internetwork must have a common Facilitation Service to control authorizations (policy) and to have them provided in a known, trusted system accessible by any application. Authorizations for both agencies and individuals should primarily be role based.

A key transition issue for the creation and successful adoption of such a control authorization module is to identify and map a commonality of authorizations among the different agencies. The stakeholders need to agree to common and minimum set of roles and hierarchies. The authorizations must be defined in the emergency response context, and must be dynamic and flexible given the unpredictability of emergencies. Reaching agreement on the commonality is a significant issue. It needs to be addressed in the governance structures, and forums will have to be established to tackle this important issue at the earliest possible time. [46]

5.4.5 Data - Ownership, Control and Access

A uniform, role-based security model is required to control who has access and update privileges to the different kinds of data flowing in the network. The ability to specify what agencies can do what is a policy mechanism, and should be enforced by a specific Facilitation Service, not by each individual application. Separating policy from mechanism is important to allow local control of data, and yet be flexible to handle unforeseen circumstances.

5.4.6 Priority Mechanisms and Related Issues

5.4.6.1 Congestion Control (packet priority)

Data and media streams will compete within the 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 control.[47] Will voice always be first? Focus Group 1D does not believe such an assertion will always

[46] Focus Group 1D notes that the National Emergency Response and Alerting Systems (NEARS) project of more than 16 national safety organizations is advocating for exactly such an approach and system. See www.nears.us.
[47] 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.

be valid.[48] 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 (e.g., incident dispatch), 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 the 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.

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 (e.g., in virtual private networks). And, as noted elsewhere, Focus Group 1D strongly encourages 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 DHS's 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.

5.4.6.2 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.[49] 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. 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.

In addition to the traffic marking and router treatment of such packets, "Call Admission Control" mechanisms can be specified and deployed 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. Preemption of lower priority sessions when higher priority sessions are

[48] 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.
[49] See SIP resource priority provisions. www.sipforum.org/; www.cs.columbia.edu/sip

initiated can be implemented. Using such mechanisms, it is reasonable to believe that the network will not become overloaded with high priority traffic. Only such traffic as the network can handle will be "admitted." 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 (e.g., high utilization with low collision rates). Focus Group 1D also cautions 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 (i.e., voice, video, text messaging) applications that have a notion of session management.

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 do. 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.

5.4.7 Managing the Internetwork: Faults, Configuration and Performance Facilitation Services

The internetwork will be composed of multiple fixed and mobile systems tied together, very much like the current telephone network and Internet. Like those, the internetwork 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 management of faults, accounting, configuration, performance, and security.[50]

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

[50] For full definitions and discussions of "FCAPS", see the following papers: http://www.sun.com/blueprints/0402/ems1.pdf (vendor paper); http://www.iec.org/online/tutorials/ems/topic03.html (non-vendor).

issues. We should learn from those experiences. Commercial networks commonly create a "Network Operations Center" (NOC). Such NOCs will be needed, which may be outsourced in some areas, and common operational procedures will be needed to allow communications failures crossing internetwork boundaries to be diagnosed and corrected.

On the other hand, Focus Group 1D explicitly does not advocate a single over-arching network management system. 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.

5.5 Agency Applications

Each agency should be free to select whatever tools they believe meet their needs, as long as they are interoperable with the Emergency Services internetwork. By creating a flow of real time voice and data communications, the Emergency Services internetwork (and local and regional networks meeting the same standards) will enable, and create a demand for, integration and decision support tools. Efforts should be made to provision for these tools and ensure that these are interconnected with the existing legacy systems. While some of them will need to be integrated in the mission critical systems, some may need to be accessed as services from the network.

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.

5.5.1 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.[51] 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 there is a rapid development of data from four sources: vehicles (telematics), personal medical information subscription services and electronic health records of all kinds, oral conversations (e.g., with PSAPs), and on-

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

scene personnel. Conjoining these data in new predictive and dynamic, algorithms will provide a powerful new tool to emergency responders.[52]

In the hazmat world, the contents, location, owner and treatment instructions (now in separate databases) could be provided to local responding agencies in real time. Then 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 (e.g., police/fire department) has a GIS system. They are often all different, with different data, different layers, different accuracy, and different coverage and incompatible formats. More comprehensive planning and implementation of GIS is needed, with more standards, and more uniform coverage.[53]

5.5.2 GIS Capabilities

Focus Group 1D notes the critical importance of another new factor: location.[54] Over and over location of emergency response elements, and the location element of data, is 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.[55]

A primary component of enhanced decision support is GIS capability. Geographic Information System (GIS) technology has been adopted widely for data display and analysis in emergency response and emergency management applications. There needs to be a basic capability available to emergency responders.

In addition, Focus Group 1D recommends sharing of geospatial information among the different safety agencies. This sharing of the different layers of geospatial information provides emergency responders with critical information to better respond to

[52] 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.
[53] The OGC is a consortium of public and private groups developing GIS standards.
[54] 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 the much larger project with far more parties discussed herein.
[55] An example of this would be violation of a geo-fence.

emergencies. Location of utility companies and their installations, building maps, location of schools, and similar information near an incident are a few examples of valuable geospatial information sharing.

There needs to be a more comprehensive planning and implementation of GIS by state and local officials with authority overall all or most emergency response agencies.[56] For data sharing, the technical issues must be resolved at the interface layer, and a valid approach must be adopted to resolve the semantics issues.

5.5.3 Application Service Provider (ASP) Model[57]

A significant hurdle for applications will be the cost and expertise involved for the necessary upgrades. Most emergency agencies are small, with limited budgets, and may lack IT expertise. Where appropriate, these can be resolved by adopting an ASP model.

The ASP model may be the most viable method to deliver the needed end user functionality in the short term to such agencies. The ability for the ASP model to spread the costs of implementation and maintenance across multiple user agencies would help defray the financial burden. The skill sets required to manage a centralized application model would not need to be duplicated at each end user agency. [58]

5.6 Policy Issues

Beyond technology, the issues discussed here require major policy processes (at every level of government), and involvement of leaders of every emergency agency in the country. Today the institutions to set the rules that the facilitation services would enforce are lacking. The institutions in the public safety wireless field are very effective for those purposes, but only extend to traditional first responders, not the entire emergency response enterprise.

Other issues 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?[59]

---

[56] The Emergency Management Mapping Application (EMMA) project by the State of Maryland is an excellent example of cooperative leadership in the GIS area. All state agencies are cooperating in providing their location-based data to a single, web-based tool, accessible to all authorized state and local emergency agencies. The next step planned is to provide access to local government GIS data.

[57] A model where-in a third-party entity manages and distributes software-based services and solutions to customers.

[58] By centralized Focus Group 1D does not intend a single centralized server, but to the contrary. The application services model will be robust and will be redundant in nature.

[59] For example, 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.

This could have profound implications for users. This is another good example of the need for new policy and protocol discussions.

5.6.1 Policies and Protocols

It is critical to establish cooperative institutions to work out new policies and protocols (network and operational) reflecting these new capabilities. Policies for access and use need to be determined by the appropriate officials.

5.6.1.1 Leadership

To achieve this vision, a lead agency needs to be identified, which will coordinate, and be responsible for assembling the parties and facilitating the decisions, tools and rules that will interconnect the disparate systems and networks. Every state / region should have a designated agency, responsible for overall emergency communications in its state / region. Where counties decide to create these networks, they must designate responsible agencies and managers to facilitate creation and interconnection of the networks. The Federal government needs to play a similar role for those tools, standards and systems that must be developed nationally.

Specific Tasks

- Secure interagency voice and data communications, connecting all emergency 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
- National and state leaders who are appointed to accomplish these goals, and given the resources to do so

While Focus Group 1D cannot see a "flag day" conversion of existing systems to the kinds of systems described here, there are few networks in place in any public safety agencies that will meet the requirements stated here.[60] 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
- Development and / or adoption of data and media standards
- Assuring a baseline capability for all emergency response agencies, including the necessary wired and wireless bandwidth

[60] 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.

- 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 entities, by other regular government budgets (e.g., transportation), and by the private sector?
- What are the statutory and regulatory barriers to achieving this vision?[61]

Since the Emergency Services internetwork is envisioned as a network of networks, a multitude of systems, and a multitude of stakeholders, it is imperative that there be national and state leadership for and of overall interoperability, and a governance structure to manage and govern the various processes. Such a structure will be successful if all the stakeholders are represented; this means all organizations involved in emergency response need to be involved, not just "first responders."[62]

The governance model should scale well to accommodate future needs, and it is vital that there is coordination among all the three levels – federal, state and local. [63]

5.6.1.2 Identification of the Statutory and Regulatory Issues

The statutory and regulatory barriers to achieve this vision need to be identified.[64] Clearly, there is no single entity responsible for developing the internetwork: the facilitation and enforcement of interoperable, inter-agency communications and coordination between jurisdictions and professions. Focus Group 1D recommends that this coordination happen at the state level, and encourages clear direction to identify the responsible entities. A national office at DHS should similarly be given the responsibility to support this.

---

[61] 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.

[62] The National Capital Region Interoperability Initiative is a primary example of an effort to accomplish many, if not most, of the recommendations made herein. It is being led by the Chief Information Officers of the diverse government entities in the region, but it has extensive practitioner involvement.

[63] Governance is identified as one of the key building blocks to achieve interoperability in Dr. David Boyd's recent Congressional testimony on interoperability. Dr. Boyd directs DHS's SAFECOM Program. It is available at http://commerce.senate.gov/pdf/boyd.pdf

[64] 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.

5.6.1.3 Funding and Funding Mechanisms

Significant new funding is required to implement the Focus Group recommendations. We strongly recommend that the FCC, Congress, the Executive Branch, states, and tribes as well as other local and private agencies work together to provide the significant additional funding needed to rapidly deploy the networks and related elements described here.

The Focus Group believes that the systems advocated in this report will greatly expand the capabilities of emergency response agencies, and indeed should produce a wide variety of efficiencies once implemented. There will be transition costs, as existing systems will not be immediately decommissioned as new ones are brought up. Bridging costs will need to be funded, as well as the upfront purchase costs. Many of the services may be able to be outsourced where the upfront expense to the government can be minimized.

There are no reliable estimates of what the costs and savings might be. However, there is reason to believe that if these recommendations are acted upon that the total societal cost of emergency response could be reduced, because of the elimination of duplicated facilities and applications now deployed for every agency, ending the duplication of data entry and the like.

Focus Group 1D believes the federal government should commission a study to determine what the costs and economic benefits of communications systems highlighted in this report might be so that there is a realistic view of what funding is needed. This study should also consider the current overall system costs – the baseline – and the costs of not making the recommended changes.

It is important that a comprehensive and inclusive study be done. Individual agency or individual domain studies will understandably only focus on the costs and benefits to that particular entity or profession. But the benefits of interoperability are systemic.[65]

5.6.1.4 Cultural Issues

The first step to interoperability is to manage and resolve the "people" issues. Given the wide spectrum of stakeholders, it is fair to expect a number of cultural issues. These have been common in American industry as it went through similar process revolutions due to advances in information technology. These include: resistance to change, fear that technology will displace jobs, learning about the needs of other emergency professions, achieving consensus, getting everyone on the same ground, inhibiting cost factors, lack of incentives to participate, lack of rewards for interoperability, and others.

[65] This is a reason why leadership by officials with broad government responsibility (e.g., governors, mayors, Chief Information Officers) is important.

Due to the absence of, or at best, minimal data sharing that occurs today, it is imperative that stakeholders understand the need for, the importance of, and the value of, information sharing. Though a great deal of progress has been achieved in the last few years, there is still a significant reluctance to change. National fire and police leaders have shown the way by coming together on a common, successful agenda to gain government understanding and resources to work toward the important goal of public safety wireless interoperability.

That success needs to be replicated for the broader emergency response enterprise, for the broader definition of interoperability the Focus Group describes in this paper. In the shorter term, Focus Group 1D recommends working on the following:

- Find strong leadership for interoperability
- Provide incentives to collaborate
- Demonstrate 'what is possible'
- Identify the added value propositions in the stakeholders' terms
- Provide collaboration tools, and document and report successes
- Institute performance milestones and metrics
- Identify multilateral solutions
- Provide federal funding to cooperative, interoperable projects, planned with all stakeholders

In the longer term, agreements will have to be in place so that the various stakeholders understand and can take advantage of the broader need and promise of information sharing. These multilateral agreements need to cover the data sharing, as well as the process sharing needs.

6 Conclusions

6.1 Vision

Focus Group 1D's vision is of ubiquitous IP connectivity. The future Emergency Services internetwork will be a network of networks, a series of separate but interconnected physical and virtual networks. This interconnection of heterogeneous networks will not only enable a faster and a more informed response, but will empower emergency agencies to have far more control over information flow and use than they have today.

The recommended technology foundation for achieving this vision, Internet Protocol, enhances existing capabilities, and enables a number of new and additional

functionalities. In order to leverage this - and if they have not already done so - Focus Group 1D recommends that the emergency agencies provision for, develop, and adopt a roadmap to achieve this vision.

The achievement of ubiquitous seamless voice communications and the promise of rich information 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, emergency communications should be moved to packet switching as rapidly as possible.[66] This will allow agencies to take advantage of the increasingly rich and diverse new information sources that 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.

6.2 Summary of Key Recommendations

Summarized below are the recommendations for each of the four questions posed to Focus Group 1D in the NRIC VII Charter, organized by those questions.

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, Focus Group 1D recommends its use. Focus Group 1D recommends:

- Use of 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.

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

- Significantly more spectrum, in large contiguous chunks, is required so public safety, indeed the staff of all emergency response organizations, can use IP efficiently when they are in the field.

- 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, in 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.

- An expedited implementation of IP architectures and systems, which will support an efficient migration path from the current systems while preserving the positive aspects of today's solutions.

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: all those that support emergency preparation or response, and the public.

    - Accommodate higher levels of interaction, managed situational intelligence, enhanced capabilities, and more comprehensive communication and coordinated response services.

- The internetwork should focus on organizations, not individuals. Organizations should be concerned about the systems that reach their members.

    - Incorporate industry safety and engineering standards for reliability, availability, and survivability. Best practices indicate redundant, physically divergent broadband 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 that achieve authentication of two participating computing platforms and encrypt

their communication to prevent unauthorized access to private information.

- 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.

- Encourage and support the development of decision support and information management tools so that responders can fully benefit from the new sources of real time data, and not be overwhelmed by them.

- 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 open, industry standards-based 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.

    - 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 databases 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) facilitation service, governed by the emergency response community. 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 agency entries and use of such registries.

- Establish a similarly governed common facilitation service 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 (for all emergency agencies) data sets, and a set of common, bi-directional emergency messages. 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 all professional response organizations can play an active 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 and require the use of interfaces that support the ability to plug in additional data services, multi-media, and voice. Minimize "one-off" systems and applications.

- Focus particular attention on developing methods to deliver the most advanced emergency information technology and services to rural areas (e.g., by sharing through ASP systems).

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 described in this report are the central nervous system of the National Incident Management System (NIMS) and a modern Incident Command System (ICS). As a practical matter they are necessary to comply with the new DHS Target Capabilities List that is the focus of DHS funding to states and localities. However, both NIMS and TCL need to provide far more specific guidance along the lines recommended in this report.

    - The primary way for Homeland Security agencies to receive appropriate data from tribal, local and state emergency agencies, and the private sector, 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 and similar clinical data. This is only possible with automated, electronic emergency response systems.

    - When there are national emergencies, external officials should be able to "listen in" to otherwise local networks. They should 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.

    - The internetwork recommended will manage first responder call out notifications, the initiation of 9-1-1 in reverse notifications to the public, and all other forms of public warning. There should not be a separate public warning network or system.

- Sharing of networks, and often applications, should be encouraged to reduce costs.

6.3 The Transition: Immediate Tasks

Focus Group 1D believes 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. Immediate transitional steps need to be taken in the key interoperability areas: Transport, Standards, Facilitation Services, Applications, and Policy. This should include the following specific capabilities:

- Fixed broadband access by the 120,000+ emergency response agencies, and the 140,000+ schools[67]
- Secure interagency voice and data communications, connecting those agencies, and allowing senior officials to immediately communicate with them with a common data messages and vice versa
- Interoperable mobile voice and data communications for emergency responders in the field
- More spectrum to enable the above
- A shared situational awareness tool (electronic maps)[68]
- Shared, non-profit internetwork facilitation service utilities and processes to make them work, including:
  - -- GIS-based registry of emergency agencies for message routing
  - -- Authentication registry and security systems[69]
  - -- System rights management utility
  - -- Network planning and management
- Common messages standards for at least the following:
  - -- Alerting of agencies and the public[70]
  - -- Real time incident status reports
  - -- Common coding of incident types and severity
  - -- Response availability for an incident in progress
  - -- Requests, commitments and status for resources of all kinds

[67] 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.
[68] Both the private sector and the Disaster Management Program of DHS have been active in developing such basic tools.
[69] 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).
[70] Note the formal approval in May, 2004 of the Common Alerting Protocol by the OASIS standards organization.

- Secure voice, data, and instant messaging between all responders, supervisors and dispatchers of all emergency agencies (e.g., intra-agency staff communications)
- Study of costs and benefits of the new internetwork
- Proper funding for the internetwork

Just as detailed talks are held about technology, there needs to be national and state leadership to launch a major parallel process of all the affected agencies. This process will have two fundamental parts: (1) establish the institutions and processes to develop and manage standards and facilitation services, and (2) 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 facilitation service utilities of the internetwork.

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.

7 Appendix A – Samples of Data Types

During Focus Group 1D's discussions, many current and future sources of data were identified as specific information that would assist emergency response agencies with their response to calls for service. The networks proposed are "all-hazard" and "all emergency." They are therefore agnostic as to which data travel over them; instead the form of data is more important: 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 Program's Statement of Requirements issued in 2004 provides a more detailed list of incident and data types.

7.1 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 an emergency communications center or 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. It should also include live video feed to responders and PSAPs, and any alarm triggered equipment response at the facility such as flushing, ventilation or release of cleanup or anti hazmat system.
- Automatic external defibrillator (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 the 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.

7.2 Real-Time Data from Private Sector Providers

- Telematics information (e.g., On Star) to include the number of occupants, speed upon impact, position of the vehicle (e.g., roll over), whether the air bags were deployed, load information (e.g., 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 (e.g., Alzheimer patients), missing children, and probation / parolees with electronic monitors.
- Burglary alarm call information, including 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 (i.e., from activation until closure of the call).
- An electronic manifest showing contents of a vehicle involved in an accident (see first bullet) with connectivity to electronic DOT Hazmat Response Guide information in both the field and dispatch.

7.3 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.

7.4 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.

7.5 Real-time Data Between Agencies and their Staff in the Field

- GPS information (x,y,z) of field units both of 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.

7.6 Non Real-Time Data from Stored Databases

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

7.7 Interactive Data

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