

INTEROPERABILITY FRAMEWORK

Emergencies demand real-time data, yet in an era when technology can bring news, current events, and entertainment to the farthest reaches of the world, many emergency response agencies cannot share data with one another — even within the same jurisdiction. Most of today's efforts to improve interoperability have been focused on wireless voice communications. While voice or radio interoperability is a critical need for responders at the scene, it represents only one side of the interoperability equation.

The Need

The National Incident Management System (NIMS) calls for an interoperable emergency data communications system linking emergency *agencies* – not just individual first responders – at all levels of government with other emergency agencies, with the private sector and with nongovernmental organizations. It is simply impossible to achieve these requirements without interoperable, interagency data communications.

Architectural Layers

There are several building blocks that must be in place to achieve effective **data** interoperability in a locality, state or region. Some of these layers are shared resources while others are components that will be unique to individual agencies. (See figure 1, which reflects the components identified in the Federal Communications Commission's NRIC VII report on the Future of Emergency Communications.) These needed layers include data *transport*, shared emergency response *standard data sets*, *enterprise services*, *emergency applications*, and the *policies and protocols* that govern the use of the system when data interoperability is achieved.

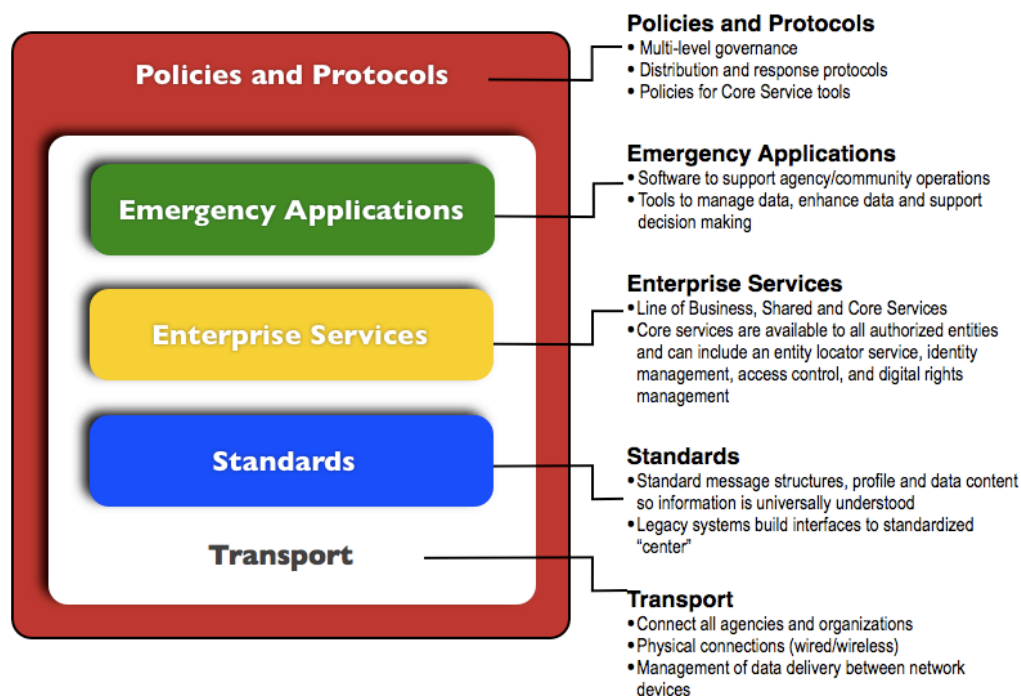


Figure 1. Architectural Layers for Achieving Interoperability

The Result

Interoperability achieved with these architectural layers enables the integration of data providers to data consumers. Agency systems as well as other discipline-specific systems can be integrated across the entire emergency response spectrum. Real time data can be collected for all types of hazards. Agencies will know immediately when an emergency event occurs. Responders will receive timely information allowing them to provide more effective response - and to reduce injuries and save lives in the process.

Transport represents the networks used for communications. This layer manages the end-to-end delivery of messages and determines how data are transferred between network devices. It manages user sessions and dialogues and controls the establishment and termination of logic links between users. The framework requires reliable and secure broadband data connections using Internet protocols.

Standards create a common language that enables data sharing between the thousands of individual agency proprietary systems being used today. With the support of the Department of Homeland Security (DHS) and COMCARE, many XML standards efforts have been launched by the emergency response community. Practitioners develop the emergency message standards and working with the vendor community these standards are field tested prior to submission to a standards body. To date, these efforts have resulted in many XML standards including the Common Alerting Protocol (CAP), the Vehicular Emergency Data Set (VEDS), and the Emergency Data Exchange Language (EDXL) suite of standards.

NLETS and public health's Public Health Information Network (PHIN).

Shared Services are horizontal services shared across one or more domains for a functionality. Examples include a shared GIS mapping system or an intelligent message broker (IMB).

Core Services are common utilities shared across all emergency response stakeholders. They adhere to a given set of requirements, rules and operating principles agreed upon by all of the domains. An agency locator and identity rights management are two such services.

By using these enterprise services, agencies do not have to spend their limited funds creating and maintaining these functions on their own.

Emergency Applications include systems such as complex Computer Aided Dispatch Systems (CAD), web-based emergency management tools, local and statewide GIS systems, hospital capacity reporting systems, and other applications. Agencies should be encouraged to purchase the tools that are best suited for them. However, it is critical that these applications all

have the ability to send and receive XML messages to other applications in standardized formats at the interface point where they connect to outside systems. It should not matter to a 9-1-1 CAD system that it is receiving data from an emergency management tool about a flood, 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 data interface should be used.

Policies and Protocols complete the interoperability framework. They determine the rights and roles of agencies in the system, and management rules for it. Does a hospital have the same

privileges as the county DOT, the 9-1-1 center, the police, or the towing company? Who has access to what data and who is allowed to send what messages? Some of these policies are already in place today. All of these policies and protocols need to be addressed by the organizations using the system before this type of architecture is deployed.

.....
For a copy of the entire Interoperability White Paper, please contact COMCARE or visit the COMCARE website.

Agency Application	CAD	EOC	Run Report	Traffic
LOB Services	NLETS	PHIN	EPA's EIEN	RHIOs
Shared Services	GIS	IMB	Information Discovery	Bio Surveillance
Core Services	Agency Locator	Identity Management	Digital Rights	Service Discovery

Figure 2. Concept of Enterprise Services

Enterprise Services are common shared tools, services and resources offered through a collective effort of the emergency response community. They enable interoperability and are available for use by authorized emergency entities. Enterprise Services consist of Line of Business (LOB) Services, Shared Services, and Core Services.

Line of Business Services are vertical, intra-domain services, such as law enforcement's