JOHNS HOPKINS UNIVERSITY/APPLIED PHYSICS LAB

Concepts on Information Sharing and Interoperability

By:

John M. Contestabile

1/21/2011

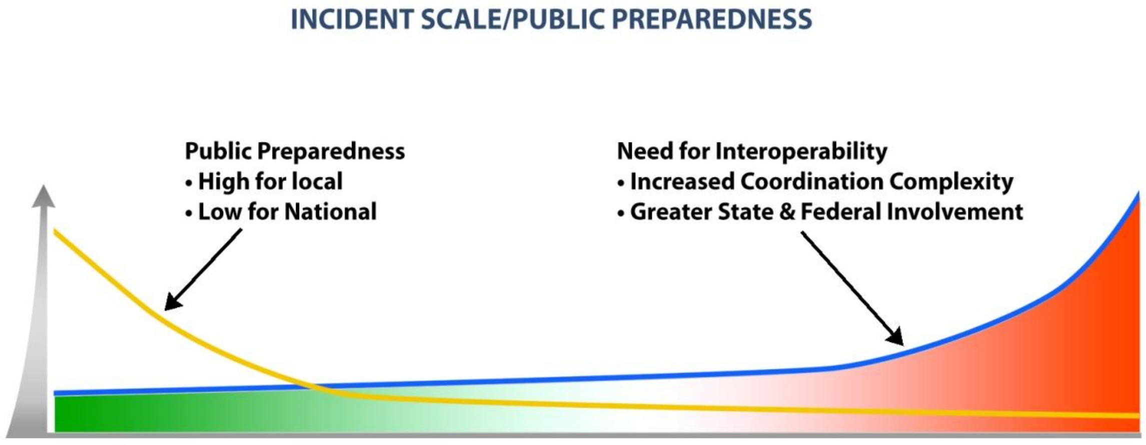
This document was prepared under an Urban Area Security Initiative (UASI) grant to the National Capital Region (NCR) from FEMA's Grant Programs Directorate, U.S. Department of Homeland Security. Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position or policies of FEMA's Grant Programs Directorate or the U.S. Department of Homeland Security.

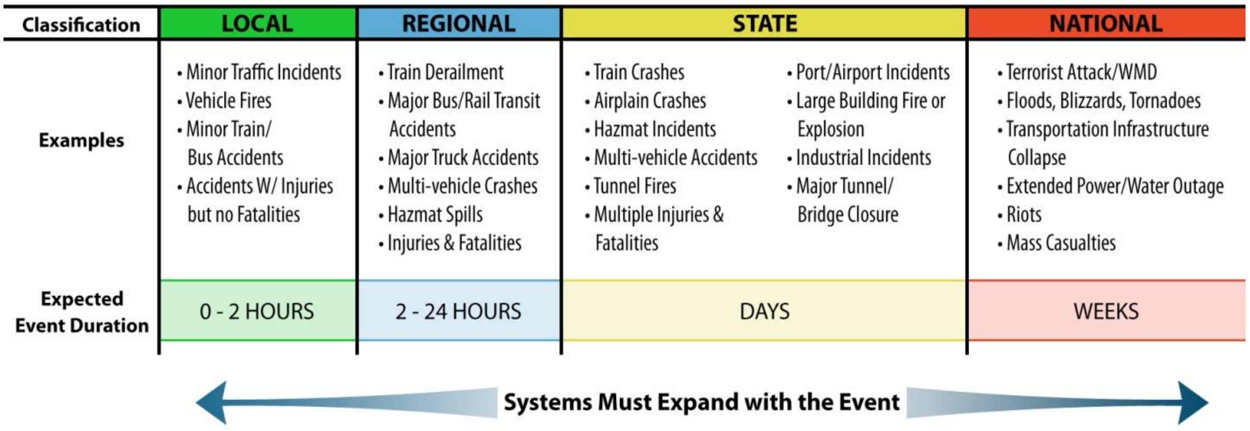
This paper addresses a conceptual framework for sharing information across jurisdictions, agencies and public safety disciplines. It was developed as part of the NCR jurisdictions (i.e. Maryland, Virginia, and the District of Columbia) interoperable communications programs. The paper explores why information sharing is important to successfully dealing with large scale events and how a lack of public safety communications systems interoperability is a major impediment. It describes a how a conceptual framework of information layers (i.e. the Data, Integration and Presentation layers) is useful to developing solutions to the lack of interoperability. It further describes a concept of operations whereby Integration layer applications can form the core of a "Common Operating Picture" which can provide information to field personnel at the scene of an incident as well as the public. Some regions of the country have implemented tools consistent with this concept (notably the National Capital Region) while elements of this concept can be found in others. An inducement for jurisdictions to participate in such an information sharing framework is that they can gain access to wide array of information to which they would otherwise not be entitled and they can reduce the overall cost of such systems by sharing the infrastructure and system expenses across the regional partners. Additionally, it is recognized that governance and security issues become increasingly important in such an information sharing environment.

Introduction

There are hundreds of thousands of incidents that occur every day in the United States, from simple/frequent incident events like automobile accidents, train derailments, theft, weather incidents, to catastrophic/infrequent incident events like the 9/11 terrorist attacks, Hurricane Katrina, the Minnesota I-35W bridge collapse and the December 2004 tsunami, to name just a few. The number of participants and resources required to respond and recover, and the complexity of their roles and responsibilities, are significantly greater and more difficult for a catastrophic incident than for a simple incident. Understanding the information needs between these different *scale* incidents will provide some insight into how various agencies and jurisdictions can better design their information systems. In short, how these systems are designed will directly correlate to the ability to share information across agencies, jurisdictions, and disciplines. That is, the design determines the systems' level of interoperability. This paper will discuss the all-hazards operational incident response and the implications for information sharing as well as propose a conceptual framework to improve interoperability based upon three layers – data, integration, and presentation.

Incident Scale and its Implication for information sharing





Classification	LOCAL	REGIONAL	STATE	NATIONAL
Examples	• Minor Traffic Incidents • Vehicle Fires • Minor Train/ Bus Accidents • Accidents W/ Injuries but no Fatalities	• Train Derailment • Major Bus/Rail Transit Accidents • Major Truck Accidents • Multi-vehicle Crashes • Hazmat Spills • Injuries & Fatalities	• Train Crashes • Airplain Crashes • Hazmat Incidents • Multi-vehicle Accidents • Tunnel Fires • Multiple Injuries & Fatalities • Port/Airport Incidents • Large Building Fire or Explosion • Industrial Incidents • Major Tunnel/ Bridge Closure	• Terrorist Attack/WMD • Floods, Blizzards, Tornadoes • Transportation Infrastructure Collapse • Extended Power/Water Outage • Riots • Mass Casualties
Expected Event Duration	0 - 2 HOURS	2 - 24 HOURS	DAYS	WEEKS

While experts can identify roles for the nation's first responder community, it is important to note that these roles are not always fulfilled on each and every incident that occurs. From an "All-Hazards" perspective, incidents vary widely, from a relatively minor "fender bender" on the Interstate highway system all the way to a terrorist event on the order of magnitude of 9/11, or a natural disaster such as Hurricane Katrina or the 2004 Indian Ocean tsunami. This Incident Scale (Figure A) schema characterizes the scope of the response to an incident as Local, Regional, State or National. This somewhat simplistic characterization will have a bearing on the number and type of agencies responding. It is within this context that a discussion of information sharing must occur as *providing relevant information to the right people in a timely manner will determine the ability to deal with the event successfully.*

Incident scale is directly associated with the level of public preparedness for a given type of incident as well as the complexity of the response coordination. For example, for the fender bender-type traffic incident, the number of responding agencies involved is quite low; often only a police cruiser and officer will respond to the scene. In this example, public preparedness is high, as the type of incident is fairly commonplace and the complexity and need for any other agency's involvement is low. Citizens typically learn of this event through radio traffic reports and a common reaction may be to "get off the highway an exit or two early", avoid the inevitable traffic tie-ups and "go home the back way". As for the first responder, the police officer would call in the license plate number to dispatch, talk with the motorist[s] involved and, barring any significant injuries, call a tow truck and perhaps stay on the scene until the truck arrives. The scene would be cleared from such an incident in less than two hours [most likely sooner] and the disruption to traffic and the surrounding communities would be minimal. This type of incident is shown as a Local incident Figure A. The few agencies involved, the minimal impact to the public, the lack of "ripple effects", and the relatively short clearance time make it a localized incident.

To continue with this example, should the license plate check [or the check of the driver's identification] surface the fact that the vehicle was stolen [or that the driver was found on a watch list of some kind – i.e. outstanding warrant, or on some sort of "person of interest" file]; the response scenario would be much different. It is likely backup forces would be called and, depending on the seriousness of the information uncovered, a police helicopter might be deployed overhead. It is also not uncommon for a lane of traffic [or more] to be closed while the vehicle and its occupants are examined. If this were the scale of the response, it would likely attract media attention and senior leaders in all the organizations involved would likely make inquiries and need to be briefed. This would necessitate additional communications efforts from the scene to "headquarters" and agency Public Information Officers [PIOs] would likely become involved.

This example illustrates the fact that incidents can rapidly become something more significant than an initial assessment may indicate. If this scenario were to occur during "rush hour" and/or the incident lasted more than two hours, it is likely that this could be classified as a Regional Event as the ripple effects on the transportation system [i.e. the resulting back up from lane closures during rush hour, those individuals that take a different route home and those that elect to take another mode of transportation as a result – take transit rather than deal with the resulting gridlock] would extend far beyond the incident scene. The time to clear the scene would be extended; the media could be covering the event "live" and system owners/operators as well as the response entities would have to provide updates and briefings. As more agencies respond to the scene, some form of incident command would have to be established. The incident scale, as this event escalates, grows.

Some incidents can be classified as Statewide events almost from the onset. For example, the threat of a hurricane, given the usual wide swath of impact, would likely be considered a statewide incident. Statewide events in this graphical schema would usually involve the activation of the state Emergency

Operations Center [EOC]. In these types of scenarios, multiple agencies are involved, incident command must be established, communications interoperability is much more important, and the need for a coordinated response across various agencies or disciplines [i.e. police, fire, EMS, transportation, etc.] and jurisdictions [i.e. town, city, county, state, and federal] is paramount. *The success or failure of the response to a statewide event is in large measure determined by how well this coordinated response unfolds in a timely fashion.*

Some events can be classified as National events. The events of 9/11 clearly were national in scope, as the air travel network was shut down for a period of time and the whole country felt the impact of the crisis. The impact of that event extended beyond the transportation system to the financial markets. Hurricane Katrina is also categorized as a national event as it affected interstate commerce and many states across the country absorbed refugee populations from the states more directly impacted. The supply chain interruptions extended far beyond those states immediately impacted for months afterward. It is in these types of national events that the federal response is most prevalent and most necessary. Events of this order of magnitude evoke the Stafford Act and a Federal Emergency Management Agency (FEMA) response. Should the event have a terrorist connection, the Federal Bureau of Investigation (FBI) as well as elements of the Department of Homeland Security [DHS] would be involved. The main point in this type of incident is that multiple agencies from the federal level to the state and local level would be involved in the response, and the communication needs become exponentially more complicated.

It is also important to note that once an event is seen as a National event, it does not eliminate or reduce the role of local, regional and state assets. As the saying goes, “all incidents are local”. That is, the local first responders will be involved at the outset and will remain involved over the life of the incident. However, additional assets will become engaged from other jurisdictions and disciplines.

This Incident Scale schema helps to frame the different types of incidents that responders and the emergency management community will face and the resultant complexities that will emerge. It illustrates that larger scale events will have communications, organizational, resource, and coordination challenges that make effectively dealing with such events problematic. While roles and responsibilities can be defined in advance, they may not be fulfilled unless the incident warrants the involvement of a particular agency or entity. And, general roles and responsibilities must be tailored to the particular event. All of this has a bearing on the need for certain types of information, who should receive it and when, how the information is transmitted and displayed, etc.

A final complication that overlies this schema is the issue of time. As mentioned earlier, incidents can escalate rapidly and become something much more complicated than first thought. For example, returning to the “fender bender” local incident, what if the vehicles involved were a passenger car and a tanker truck carrying hazardous materials? And, what if the tanker truck was damaged in such a way as to begin leaking product that created a plume, threatening a nearby school? The challenges to respond promptly, size up the situation, establish communications, establish a command structure, obtain weather information, warn and evacuate [or shelter in place] the school and neighborhoods involved are enormous. In a moment a single variable in an otherwise common, local incident can make time the critical factor on which lives depend.

The thinking of incidents as local, regional, statewide, or national helps responders and other involved agencies/jurisdictions grasp the inherent complexities as one moves from left to right on the graphic as an incident escalates. *Those agencies and jurisdictions require established communications and command and control systems that are able to adapt as quickly as the event itself may escalate.* Understanding roles and responsibilities in this context will help those involved to recognize the limitations and challenges of current systems and identify gaps where improved protocols, communications systems and resources are needed. *Successfully dealing with an emergency incident involves getting the right information to the right people at the right time.*

Public Safety Communications Interoperability

A significant barrier to getting information to those that need it in a timely manner has been referred to as a lack of communications "interoperability"
[See: http://www.safecomprogram.gov/SAFECOM/interoperability/default.htm].
That is, systems that cannot share information readily with other systems. These systems could either be voice communication systems [such as an 800 MHz system user that cannot talk with a 450 MHz system user because of the different frequency bands] or data systems [such as Geographic Information Systems – GIS, Computer Aided Dispatch Systems – CAD, or Traffic Incident Management Systems – TIMS, to name a few, that utilize different data formats, programming code, or lack standards for information sharing]. This lack of interoperability among systems impedes the flow of information across jurisdictions [e.g. from a county EOC to a State EOC], agencies [e.g. from the Department of Motor Vehicles to the local police field units], and disciplines [e.g. between police and EMS].

So, if the Incident Scale discussion illustrates that sharing information across jurisdictions/agencies/disciplines is key to successfully dealing with larger scale events, and that information sharing is impeded by a lack of interoperability of the communications systems involved, then reducing the causes of interoperability should improve information sharing. However, reducing interoperability problems is much easier said than done, for numerous reasons. There has been much effort put into this problem over the past several years, including the naming of Statewide Interoperability Coordinators [SWIC's], the development of State Communications Interoperability Plans [SCIP's], targeted grant programs [Interoperable Emergency Communications Grant Program -- IECGP, for example], as well as the publication of considerable federal guidance
[See: http://www.safecomprogram.gov/SAFECOM/].

One of the reasons solving the interoperability problem has proven so difficult is that *it is not solely a technical problem*. Agencies have not purposely built systems that would not work with other systems, but rather they built systems to meet their particular business needs within normal budget limitations. If it was not determined to be a critical need to share information with another agency, then scarce dollars were not allocated to providing that connection. And while that may be true for a Local event [as discussed above], that does not hold true if the event scale could be considered a Regional, State or National event. In those cases, sharing information widely is key to successfully responding to and recovering from that event. So, a lack of interoperability remains an issue in existing systems [and even in planned systems] because of a *lack of perceived need to share information widely* [since an agency may only participate in more than a localized event only a few times a year] or because of *insufficient funding* to adjust the project to make the system more interoperable.

In addition to a perceived lack of need or lack of funds to build a more interoperable system, there are several other factors that need to be considered. The Department of Homeland Security "Safecom"

Program has identified five factors that have a bearing on interoperability: Governance, Standard Operating Procedures, Technology, Training and Exercising, and Usage.
[See: http://www.safecomprogram.gov/SAFECOM/tools/continuum/default.htm] The "Interoperability Continuum" illustrates that there are degrees of interoperability and that some progress across all these factors must be made in order to improve interoperability.

While the Continuum is quite useful in understanding the impediments to interoperability, it is not detailed or specific enough to provide a framework for achieving interoperability. While very specific details must be left to the locale in which interoperability is being addressed [that is, the governance, standard operating procedures, technology, etc. in that area], a technical framework for achieving interoperability can be articulated. The remainder of this article hopes to provide a framework for achieving data interoperability.

How might communications interoperability be achieved during emergency events?

As mentioned above, solving the interoperability problem is not just a technical issue. All too often money has been spent on a technical solution [a "black box" solution] only to find that the solution does not meet the need of end users. This matter is more than the technologists doing a better job of requirements gathering. Solving the interoperability challenge involves navigating human relationships and issues of trust and must be approached in that fashion. The importance of trust has been raised in many forums [see the All Hazards Consortium: www.ahcuas.org for example] and the lack of which will impede information sharing. Recognizing these challenges, *some success can be had if the problem is approached sequentially from a people, process and technology standpoint.* That is, the *people* from different jurisdictions/agencies/disciplines must come together and work through a *process* whereby they can understand each other's need for information, and trust can be developed between the parties. Only then can a *technology* approach/solution be identified and applied. Often times, grant deadlines, consultant schedule constraints, preconceived notions as to the "right" solution and a general lack of understanding of this dynamic work against giving the people and process steps sufficient time to develop a creative and workable technical solution.

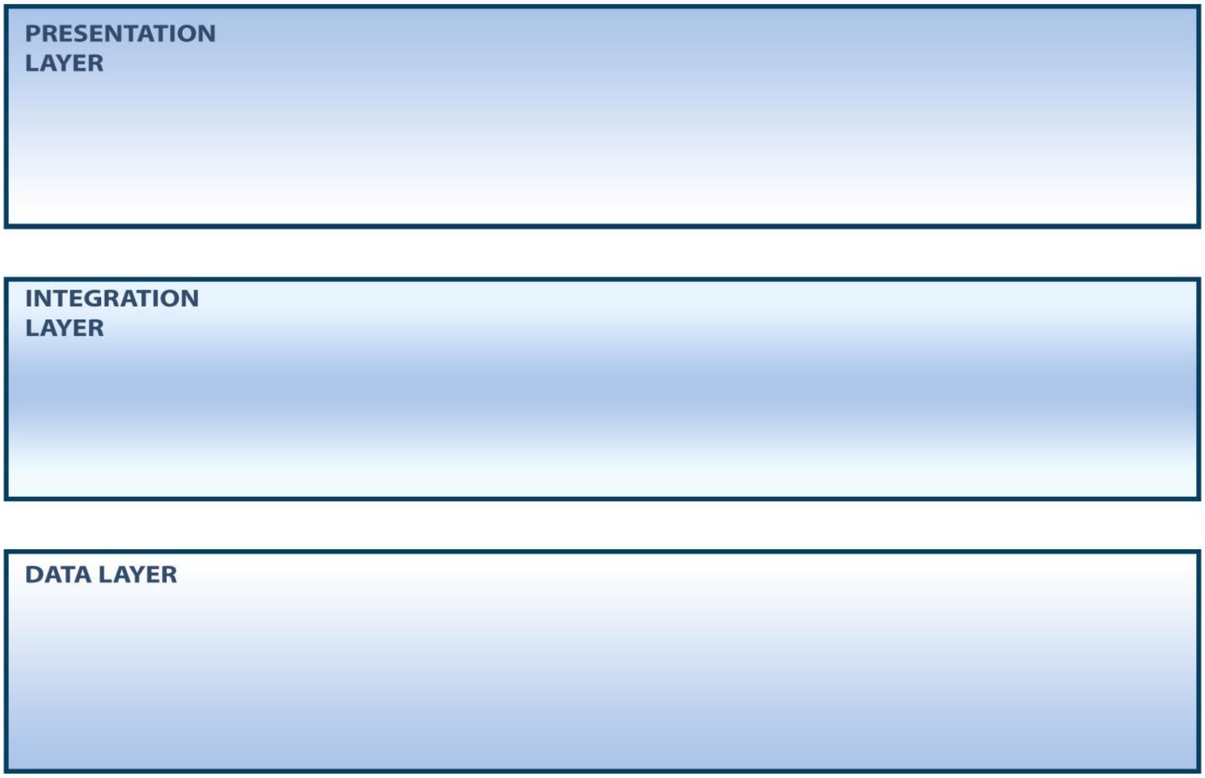
While solving the interoperability challenge is not solely a technical matter, technology is still an important part of the solution. In fact, there is a dynamic between technical and non-technical factors that is somewhat symbiotic. It is all too easy for the participants in the process to pay lip service to sharing information if they know that there is no technical way for them to do so. Once a technical approach has been identified [if not actually applied], the participants must own up to the commitment to share data by investing and working toward the solution. This is the turning point in the process when the participants have the "ah ha" moment and identify an approach, architecture or solution that everyone can buy into, which creates conviction and momentum. Only then will the project have the potential for success.

To summarize, successfully dealing with larger scale events requires sharing information widely and a lack of interoperability between the systems that hold that information is a major impediment to success. There are factors beyond the technology that have a bearing on solving the interoperability challenge and the people who have the need to share information must work through a process of discovery to identify an appropriate solution that works in their setting. Experience in developing solutions in this space suggests that there is a pragmatic approach to this problem that is applicable in most settings. The proposed conceptual framework that follows would provide for improved information sharing that could link various operation centers as well as field units at the scene of an incident.

A Conceptual Framework for Information Sharing and Improved Interoperability

Consider a conceptual interoperability framework in which there are three levels that can be applied to most settings where interoperability is desired, and can be achieved with minimal impact to existing systems. The three layers comprising the framework include:

- The *Data Layer*,
- the *Integration Layer,* and
- the *Presentation Layer*.



The Data Layer

At the bottom of the graphic lies the data layer where all the various data sets and applications spread across various jurisdictions/agencies/disciplines reside. Local data sets [for example, property patterns, zoning, locations of fire hydrants, school building plans, crime statistics, water supply and storm water systems, etc.], regional data sets [such as traffic network volumes, landfill information, wastewater treatment systems, etc.], state data sets [such as health records, social services, state roadway data, environmental information, etc.] as well as federal data sets [such as geospatial, aerial imagery, crime statistics, for a more comprehensive list of examples see: www.data.gov]. While the location of this data can vary from place to place [that is, which agency or jurisdiction is responsible], there is no doubt this data exists in every location and that some agency is responsible for creating it, tracking it, and maintaining it for some legitimate business purpose. Typically, these systems lie behind agency firewalls, were built with some level of customized code [even if off the shelf software/applications were used], and are designed for agency use, not designed to share information with others outside the agency or beyond the firewall. In fact, Chief Information Officers [CIO's] of these agencies are often unwilling to share information from these systems to others outside the firewall because of costs and legitimate security concerns. Additionally, in the case of public agency data systems, these systems are often older, large, complex systems [think of driver's license, health care and voter systems for example] in which CIO's are wary of creating interfaces to other agencies for fear of the effect it will have on the stability of the rest of the system.

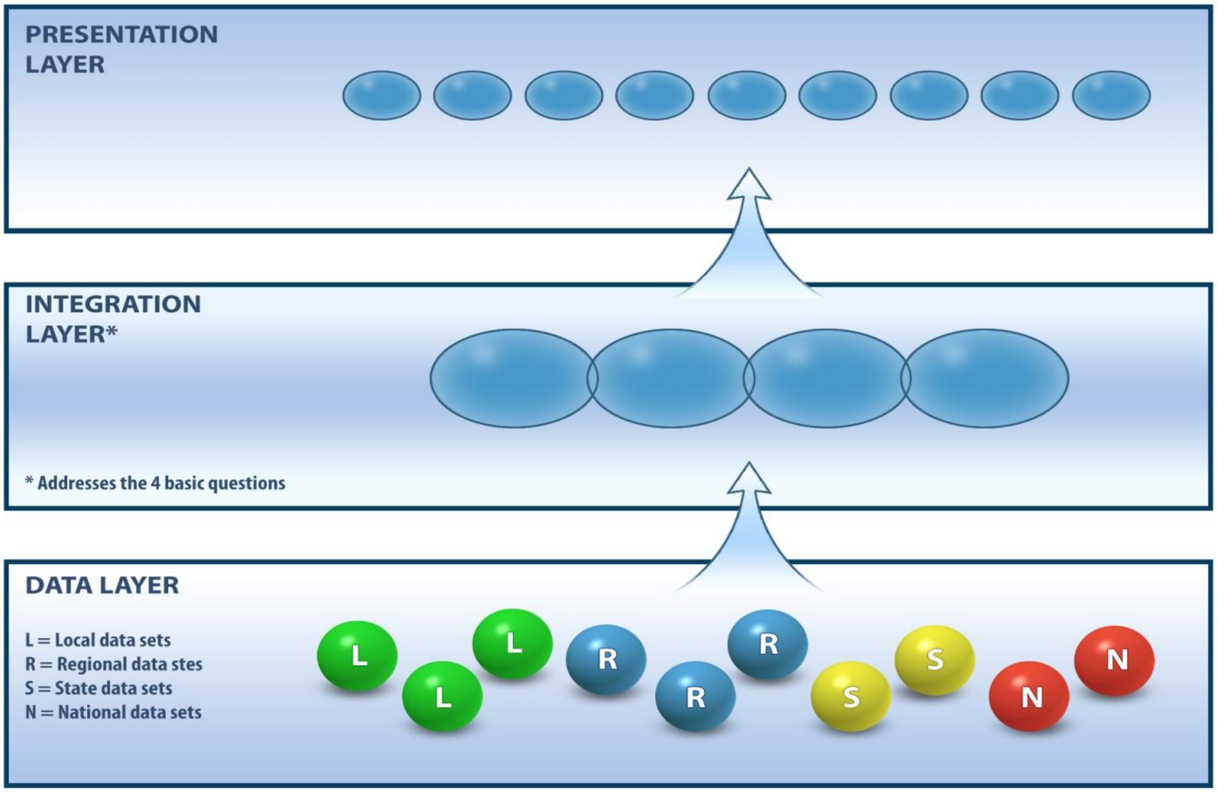
One method of improving data sharing would be to create interfaces between all the disparate systems at the data layer but, for some of the reasons noted above, this is problematic. Additionally, if one were to provide for interoperability at this layer, it would result in a multitude of "one off" connections. For example, if county police agency A wished to share information with an adjoining county B they could build a custom interface between their systems. If county police agency C wanted to also see that information, an interface would have to be built with that agency, and so on. Ultimately, there would be multiple different interfaces between each of the agencies who wanted to share information. One can appreciate how a CIO would not embrace this approach by having to develop, fund and support multiple interfaces to their same system.

The Integration Layer

A more artful approach, in keeping with today's networked architecture, would be for those data layer systems to publish *once* to an integration layer tool. Those agencies/jurisdictions and disciplines who need to see that data, could now look to the integration layer tool to see that information linked to other agencies with like data. To return to the previous example, police agencies A, B and C would all publish their data once to an integration layer tool so that if any of the agencies desired to see any of the other agency's data, they would look to the integration layer tool; not to the other agency. Done properly, this would be transparent to the individual agency; that is, each agency would still use their native system but the results would be published to the integration layer tool out of the "back end" of the system.

Of course, publishing data from the data layer to the integration layer would need to respect *network protocols*, *security requirements* and the appropriate *standards* for that data. The concept would be to publish the data out of the typically proprietary, customized, legacy/mainframe environment from which it came [in the data layer] into a web enabled, Internet Protocol (IP) and standards based, open environment [in the integration layer].

With data having been published into the integration layer, *interoperability can then be achieved by connecting the various tools found in that layer.* Since these tools are more amenable to integration, they can be connected and data can be shared across these tools so that it can be seen in a larger context. Unlike trying to achieve interoperability at the data layer, providing only a few interfaces between a handful of key integration tools is feasible. The presentation of this three layer schema can be seen in the graphic below:



<u>What tools should be provided in the Integration layer?</u>

This question is akin to asking what data is needed during an emergency. While one cannot give a complete answer due to the unique information sharing needs of each incident, there are certain information needs which are almost always required. *Typically, four questions need to be answered:*

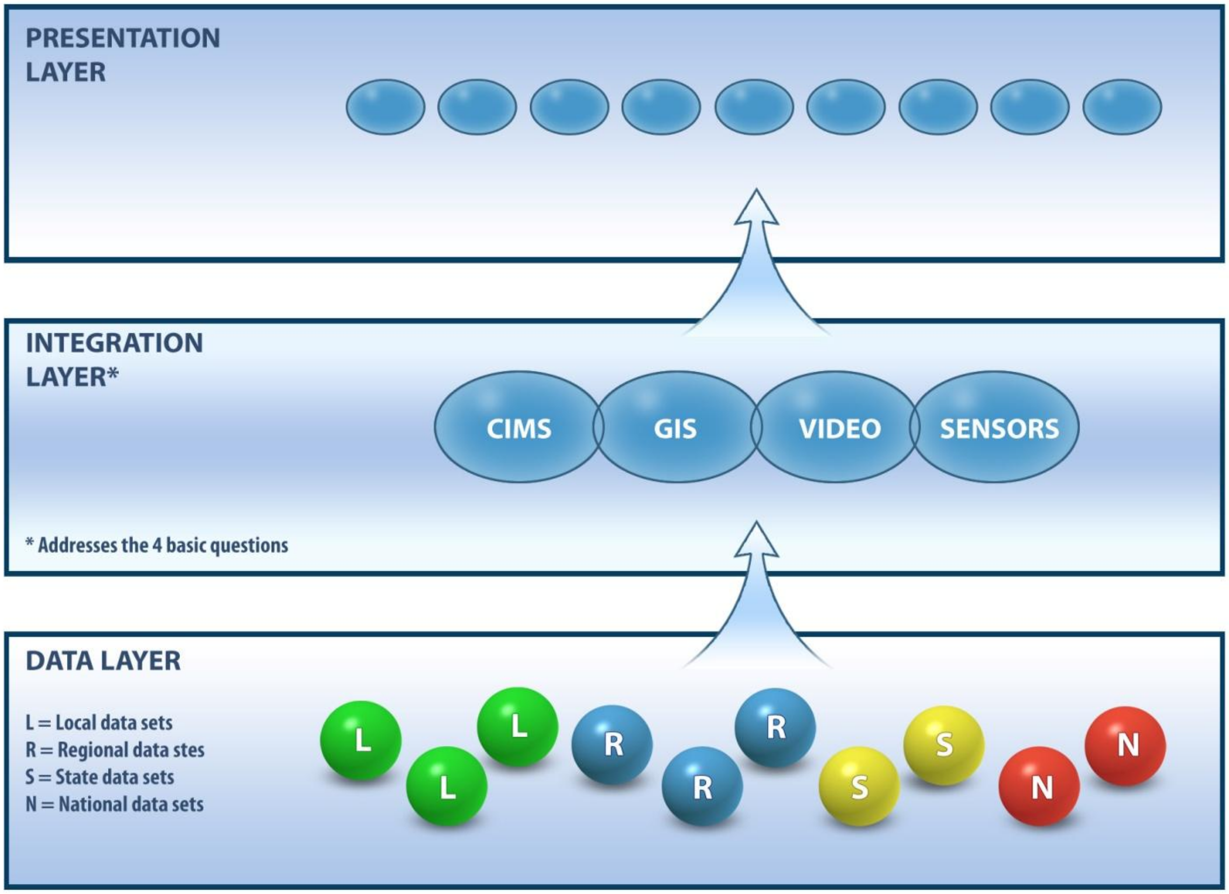
1. Where is it?
2. Can we talk about it?
3. What do we know about it?
4. Can we see it?

These questions have ramifications for four types of data or capabilities:

1. Geographic Information Systems (GIS)
2. Voice Communication Systems (as well as Critical Incident Management Systems – CIMS)
3. Access to disparate data sets (such as sensors)
4. Video systems

Thus, *the Integration Layer tools must address (at least) the four types of desired data: GIS, CIMS, Sensors, and Video - as well as other data sets.* Some sort of application or tool that can "ingest" information of that type and aggregate it with other like information as well as share it horizontally with the other tools in the integration layer is what is needed. Additionally, now that the disparate data has been aggregated and integrated, it may be necessary to overlay *analysis and decision support tools* to make better sense of this wide ranging set of data.

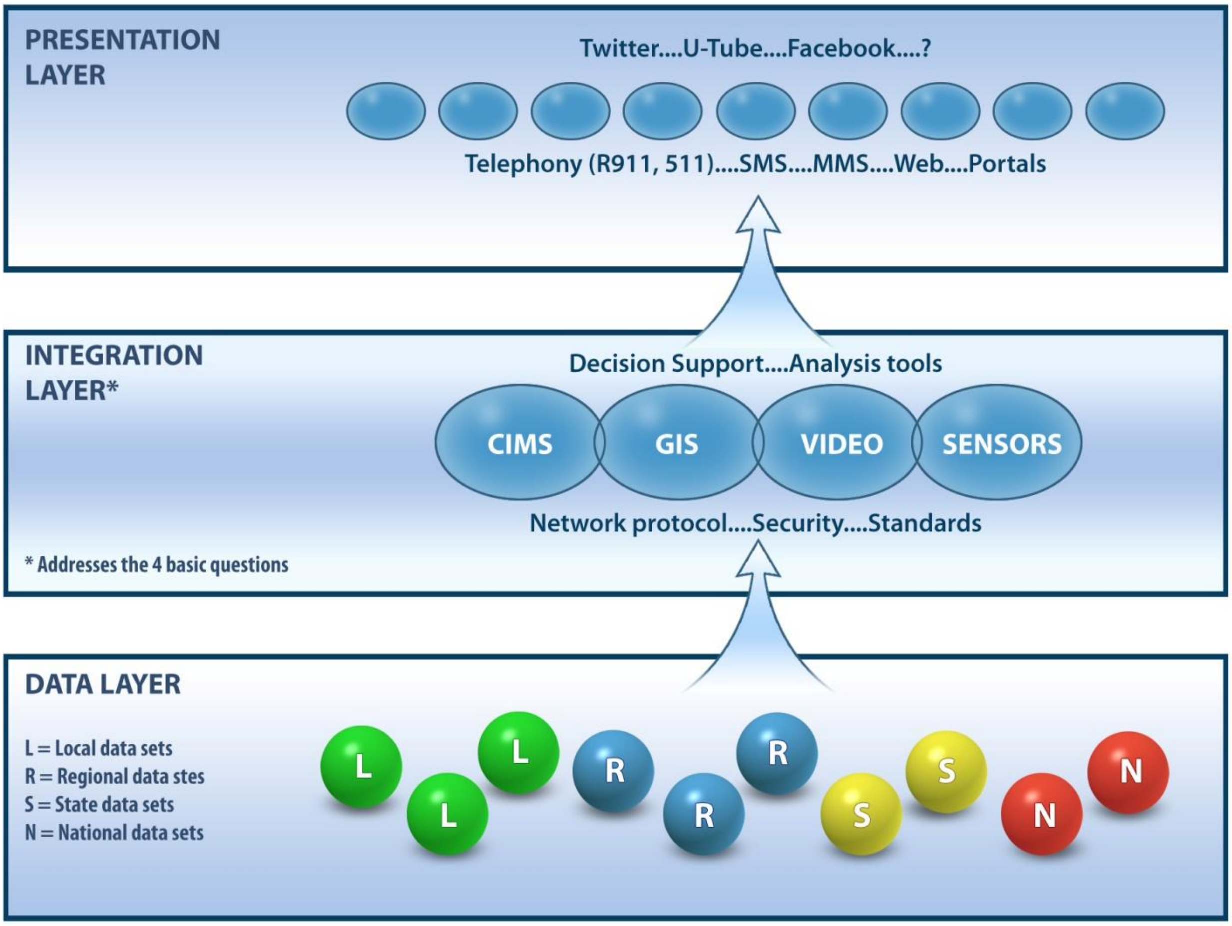
Revisiting the Conceptual Interoperability Schema graphic, the integration layer tools could be labeled as noted below.



The Presentation Layer

Now that the data has been published into a handful of integration tools and *those tools have been connected to achieve interoperability*, the fused data needs to be "served up" to allow visibility across agencies/jurisdictions and disciplines by *publishing into the presentation layer using a variety of channels;* from telephony, to web based, to Short Message Service [SMS], and Multimedia Messaging Service [MMS]; both wired and wireless.

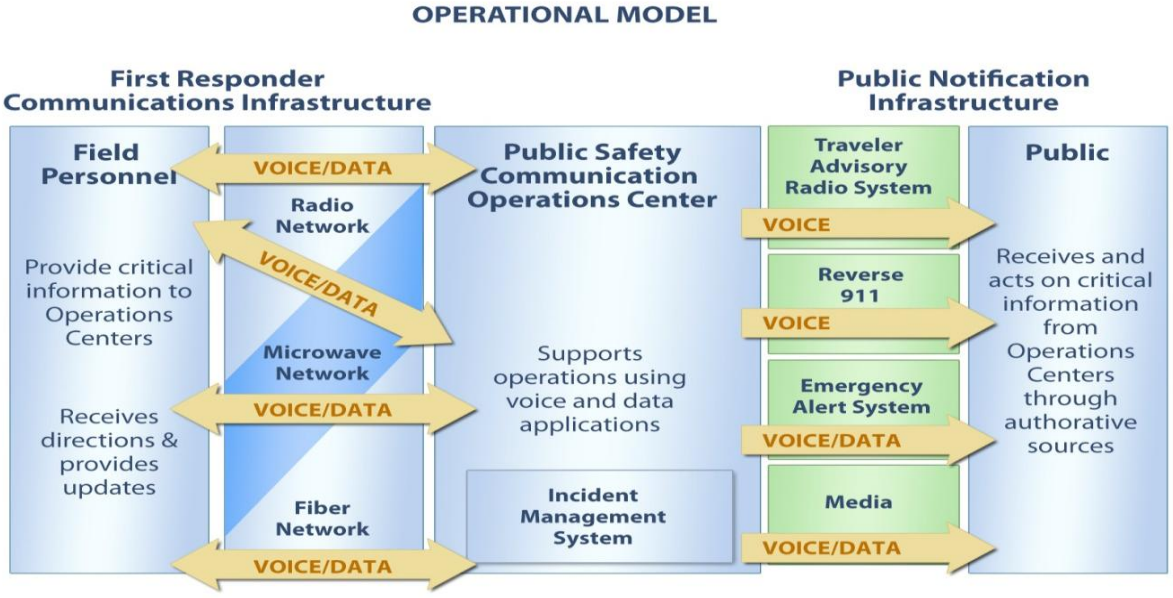
This will allow the information to be delivered to those that need it [via push and pull methods] across emergency operation centers, incident command posts, responders as well as the public. The presentation layer can be used to *distribute the information beyond the data owners* that have provided it to the Integration layer and can *take advantage of existing social networking tools* to extend their reach.


PRESENTATION LAYER
Twitter....U-Tube....Facebook....?
Telephony (R911, 511)....SMS....MMS....Web....Portals
INTEGRATION LAYER*
Decision Support....Analysis tools
CIMS
GIS
VIDEO
SENSORS
Network protocol....Security....Standards
* Addresses the 4 basic questions
DATA LAYER
L = Local data sets
R = Regional data stes
S = State data sets
N = National data sets
L
L
L
R
R
R
S
S
N
N

Operational Model

With such an information sharing schema in place, the participating partners/agencies that provide information to the integration layer can then see their information in relationship to the other partners. For example, the GIS tool would show the location of incidents listed in the CIMS software log as well as links to the video cameras and other sensors in the vicinity as well as across the region. The GIS tool would also have multiple layers of the information available on roadways, schools, shelters, evacuation routes, transit/rail systems, parks, utilities, critical infrastructure, etc. This tool could form the basis of a Common Operating Picture [COP] which all the partners could see; with information updated and published in near real time.

Given that this suite of integration tools would have the most up to date information during an incident; this COP could be the information sharing engine that bridges operations centers and field units at the scene of an incident. Today, there are many variety of operations centers [such as State/County/Municipal Emergency Operations Centers (EOC), Traffic Management Centers (TMC), Fusion Centers, as well as utility companies and transit Operations Control Centers (OCC)] functioning on a 24x7x365 basis. However, there is typically no common software platform(s) to which they can all look to have a shared understanding before/during/after an incident. The integration layer tools would provide a COP and, as such, a vehicle for collaboration across centers and a method to respond to requests for information from the field units. This information sharing framework would be a way to engage these various centers in supporting the field personnel and the incident command system while providing a much needed collaboration tool and COP. Such a conceptual Operational model can be seen below.


OPERATIONAL MODEL
First Responder Communications Infrastructure
Public Notification Infrastructure
Field Personnel
Provide critical information to Operations Centers
Receives directions & provides updates
VOICE/DATA
Radio Network
VOICE/DATA
Microwave Network
VOICE/DATA
Fiber Network
VOICE/DATA
Public Safety Communication Operations Center
Supports operations using voice and data applications
Incident Management System
Traveler Advisory Radio System
VOICE
Reverse 911
VOICE
Emergency Alert System
VOICE/DATA
Media
VOICE/DATA
Public
Receives and acts on critical information from Operations Centers through authorative sources

While the discussion above relates the possible uses/benefit to the various operations centers and field personnel, this suite of tools in the integration layer also would provide benefit to communicating with the public. Selected information from this suite could be published to the presentation layer and distributed via:

- the web and/or various social networking tools
- telephonically through reverse 911 or 511 or SMS
- Traveler Advisory Radio [TAR], or the proposed
- Integrated Public Alert and Warning System [IPAWS]

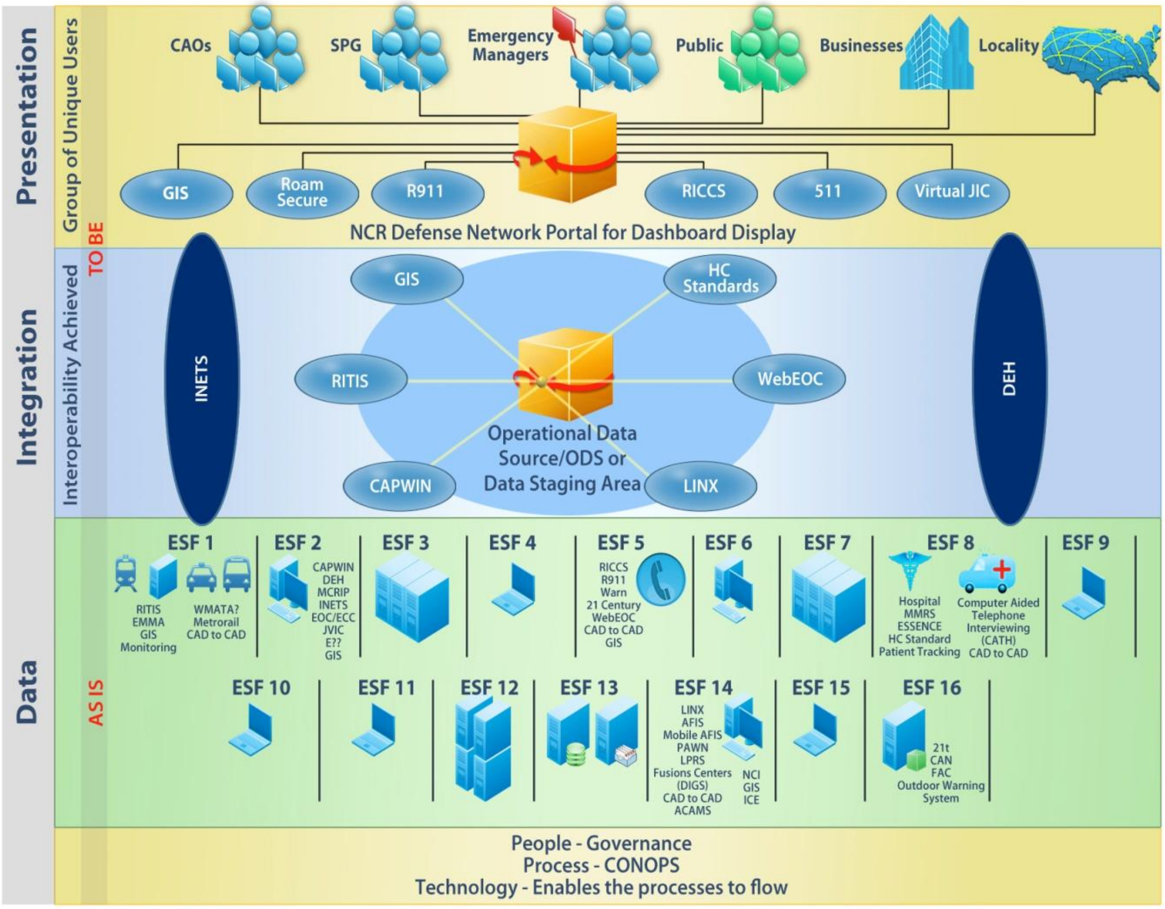
These varied methods of information distribution via automated means would speed the dissemination of authoritative information to the public during incidents when timely and accurate information sharing is critical.

Efforts to Implement the Conceptual Framework

Some jurisdictions are building systems/solutions that comport to this Conceptual Interoperability Schema. For example, the National Capital Region [NCR, which includes the District of Columbia, Northern Virginia and a portion of Maryland], using Urban Area Security Initiative [UASI] funds, has put in place many tools in the integration layer to achieve information sharing. They have also investing in developing a region wide fiber network [called the NCRnet] and protocols for information sharing [called the Data Exchange Hub – DEH]. Information on NCRnet and DEH can be found at www.ncrnet.us .

An original graphic (developed by others in the mid 2000's) depicting these applications organized within the conceptual framework can be seen below. Regional tools such as LINX [Law enforcement Information Network Exchange], WebEOC, RITIS [Regional Integrated Transportation Information System], CAPWIN [Capital Wireless Information Network], HC Standard and a regional GIS tool are all integration layer applications that aggregate like information from the data layer for a variety of end users. These applications are connected [in some cases] and plan to use the NCRnet and DEH for transport so as not to rely on an internet connection during emergencies. Some of the presentation layer tools are in place, such as Roam Secure/RICCS [see: http://riccs.mwcog.org/faq.php], but much of this layer of the framework is still being built out.

NATIONAL CAPITAL REGION INFORMATION SHARING FRAMEWORK



What are the benefits and challenges?

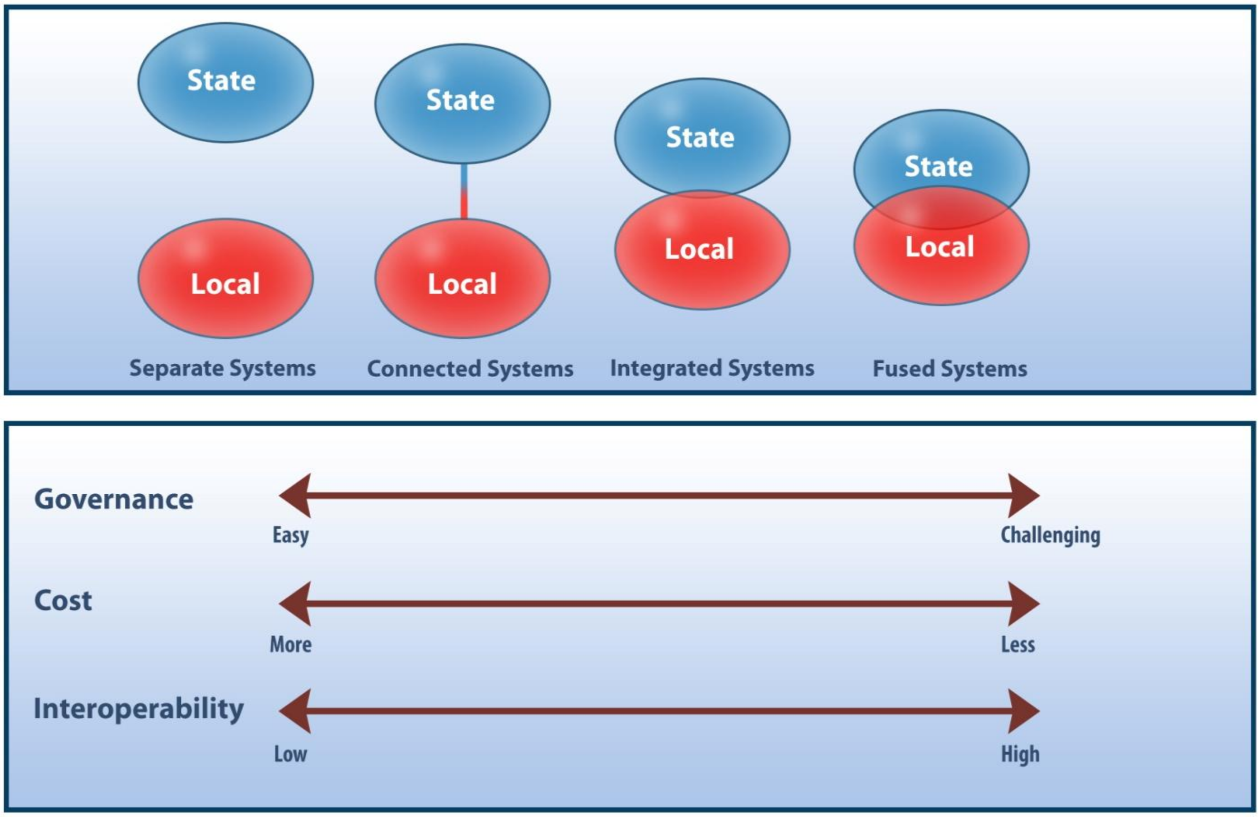
The *benefits* of developing information sharing systems according to this conceptual framework are that participating agencies will have access to a wealth of information in the integration layer upon which to make better decisions before, during and after an emergency incident. Incident commanders are routinely challenged in most every emergency incident they face to make decisions in the absence of information and, while it would be naive to think a commander would ever have all the information needed, such a schema would improve considerably the information at his/her disposal. Additionally, this information may help save lives [of both responders and victims] and time [to formulate decisions and take actions]. Additionally, this approach allows agencies to continue to use their legacy systems in the data layer, while taking advantage of other tools/applications in the integration layer for improved situational awareness.

The *challenges* are that it requires agencies/jurisdictions and disciplines agree to share their data as well as fund and share the needed integration layer tools. As noted above, this requires that those involved see the need to share information and develop a certain level of trust that they can do so in a secure fashion. Regarding funding, another challenge is that integration layer tools are shared, and yet we continue to budget funding by agency and jurisdiction. Regional grant funding has been able to bridge that gap, yet ongoing funding for sustainment can be a challenge without commitment from the participants.

The *incentives* for information sharing are that costs can be driven down by sharing infrastructure/systems and pooling resources. The graphic below illustrates that interoperability improves as systems evolve from *separated* to *connected* to *integrated* and ultimately *fused* systems. But, as systems become more connected, *governance* becomes increasingly important. With shared systems, an individual agency's ability to make changes to that system is constrained and a mechanism to adjudicate disputes must be in place. There may also be a need for memoranda of understanding [MOU] or agreement [MOA] to set up the necessary governance and ongoing funding.

While the benefits of this information sharing framework are potentially quite considerable in information availability and cost savings, the obstacles of governance, agreements and long term funding are likewise formidable.

BENEFITS AND CHALLENGES OF INTEGRATED SYSTEMS CONTINUUM



Summary

- The ability and speed with which you can share information across agencies/jurisdictions and disciplines during an emergency will determine how well that incident will be managed. This is why communications interoperability is important; as it is the key impediment to sharing information across the various incident stakeholders.

- Achieving interoperability at the data layer, by connecting systems/data sets at the individual agency level is not prudent, scalable, manageable or realistic. Thus, creating an integration layer with a handful of key applications/appliances which can consume published data [in near real time, optimally], is the strata at which interoperability can be achieved.

- Of course, publishing into the Integration layer must respect network requirements, appropriate standards for the data being published and security. The data owner must be able to set the security level of their data, and thus which users can view that data.

- Once the data is consumed into the Integration layer, it is shared across the other applications so as to achieve interoperability and contribute to a more complete operating picture during an incident. Analytical and decision support tools are also useful in this layer to bring key information to the decision makers attention.

- Benefits of creating an integration layer are: access to data across agencies/jurisdictions and disciplines, improved interoperability, and potentially reduced cost overall. But, it is recognized that governance becomes more important in shared systems.

- Applying these concepts to any particular region will result in some variation, but the National Capital Region has built many of its existing systems consistent with this model.

- The presentation layer is important to distributing the integrated data to end users and leveraging private resources [such as social networking tools]. While examples can be found of the data and integration layer concepts, development of the presentation layer remains largely underdeveloped at present.