# NPSTC Quarterly Newsletter

*Volume 11 Issue 3, Fall 2011*

*NPSTC Home*

## From the Chair

*by Ralph Haller*

In November at the RCA Annual Awards Banquet, NPSTC will present the 2011 Richard DeMello Award to NPSTC's Executive Director, Marilyn Ward…

## Well-Deserved Congratulations to Marilyn Ward, 2011 DeMello Award Winner

From the Florida Highway Patrol to dispatch to renowned national leader in public safety telecommunications, "Her untiring devotion to improvement of public safety communications has resulted in numerous rule changes at the FCC, all favorable to public safety," says Chair Ralph Haller…

## Concepts on Information Sharing and Interoperability

*by John Contestabile*

This paper addresses a conceptual framework for sharing information across jurisdictions, agencies, and public safety disciplines…

## Next Generation 911 What's Next Forum

Prepared by the Transportation Safety Advancement Group (TSAG), When a major traffic accident occurs on the highway, local 911 centers receive increased numbers of calls alerting them of the accident. When NG911 is widely available, how will the PSAPs manage the volume of text messages they are sure to receive?…

## Science and Technology Directorate Wins Two Awards for Cyber Security

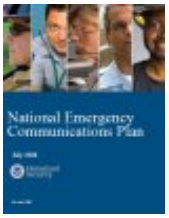
*Posted by Doug Maughan, Director, Cyber Security Division, DHS Science & Technology Directorate*

DHS's Science and Technology Directorate receives two awards for work in strengthening the nation's cyber security posture…

## OEC Showcases Successful Implementation of the Interoperability Continuum

To highlight advancements made by stakeholders, OEC published five case studies in September 2011 that align with the SAFECOM Interoperability Continuum…

## NECP Update from Office of Emergency Communications




More than 85 percent of the NECP milestones have been achieved to date, and progress is evident in all of the NECP priority areas, such as governance, training, and coordination…

## Remember the Past, Honor the Future - 9/11 Tribute

On September 11, 2011, NPSTC posted on our home page this tribute to public safety and to all who lost their lives…

## Regulatory Update

*by Bette Rinehart, Editorial Task Group Chair*

The FCC has released an NPRM asking for comment on the best ways to encourage deployment of technologies that will allow consumers to send texts as well as other non-voice information to PSAPs using 911…

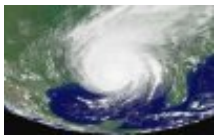
## Message from the Public Safety Communications Research (PSCR) Program

*by Dereck Orr, Program Manager for Public Safety Communications*

PSCR's 700 MHz Public Safety Broadband Demonstration Network project continues to make progress, with more than 9 vendors installing and testing equipment…

## ESF-2 Working Group Ready to Roll

## Virtual USA: The Right Information, at the Right Time, for



Emergency Support Function-2 (ESF-2) has played a very important role providing communication services to disaster victims during Hurricanes Katrina and Rita…

### the Right People

In an emergency, reliable information is a decision-maker's most important asset…

### WinnF Needs Input for Technology Report to Guide Purchasing and Research Agendas

The Wireless Innovation Forum [formerly Software Defined Radio Forum] has issued a Request for Information on current and proposed technology developments for addressing public safety communications requirements…

### Since We Last Met

PSCR Releases In-Building Systems Document, Canada Holds Fifth Interoperability Workshop, GPS Update, LightSquared Update, NPSTC Filings, and more…

Important Dates *(click here for NPSTC Calendar of Public Safety Events)*

| Date | Event | Location |
|---|---|---|
| **NOVEMBER 2011** | | |
| November 2–3 | ISC Solutions | New York, New York |
| November 3–6 | Society of American Foresters National Convention | Honolulu, HI |
| November 6–9 | APCO Canada 2011 Conference | Ottawa, Canada |
| November 12–17 | IAEM 59th Annual Conference and EMEX 2011 | Las Vegas, NV |
| November 28 | NPSTC Quarterly Committee Meeting | Teleconference |
| November 30 | FCC Open Commission Meeting | Washington, DC |
| **DECEMBER 2011** | | |
| December 4 | Canadian Social Media for Emergency Management Tutorial | Ottawa, Canada |
| December 4–7 | CITIG 5th Public Safety Interoperability Workshop | Ottawa, Canada |
| December 6 | SAFECOM National Council of SWICs Emergency Comm Intergovernmental Roundtable | Atlanta, GA |
| December 7–8 | National Council of SWICs | Atlanta, GA |
| December 8 | NCSWICs EC | Atlanta, GA |
| December 13 | FCC Open Commission Meeting | Washington, DC |
| **JANUARY 2012** | | |
| January 16–20 | Radiocommunication Assembly 2012 | Geneva, Switzerland |
| January 17–19 | International Disaster Conference and Expo 2012 | New Orleans, LA |
| January 18–21 | NSA 2012 Winter Conference | Washington, DC |
| January 23–31 | ITU World Radiocommunication Conference 2012 | Geneva, Switzerland |

Publication Information

*NPSTC Quarterly* is the newsletter of the National Public Safety Telecommunications Council (NPSTC). NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership. Funding for the NPSTC newsletter is provided by the Department of Homeland Security, Office for Interoperability and Compatibility (OIC) and the Office of Emergency Communications (OEC). We welcome questions, comments, and story ideas. Please contact the Support Office at (866) 807-4755 or by email at support@npstc.org.



## From the Chair

*by Ralph Haller*

In November at the RCA Annual Awards Banquet, the National Public Safety Telecommunications Council (NPSTC) will present the 2011 Richard DeMello Award to NPSTC's Executive Director, Marilyn Ward. From the Florida Highway Patrol to dispatch to renowned national leader in public safety telecommunications, her untiring devotion to improvement of public safety communications has resulted in numerous rule changes at the FCC, all favorable to public safety.

Beginning in 2005, NPSTC has presented an annual award to one public safety communications person who has demonstrated the highest levels of personal and professional conduct and performance in the local, state, and national public safety communications arena. The Richard DeMello award was named to honor the achievements of DeMello, one of the founding fathers of NPSTC. He was a frequency coordinator for the Forestry Conservation Communications Association (FCCA), the 700 MHz Regional Planning Committee Chair for Region 21, Michigan, a Life Member of the Association of Public-Safety Communications Officials – International (APCO), and a member of RCA. Marilyn was one of the founding members of NPSTC as well and its first Chair. Read more about her accomplishments in *Well-Deserved Congratulations to Marilyn Ward, 2011 DeMello Award Winner*.

NPSTC hosted its fall quarterly meeting in late September in Orlando, Florida. As always, it was a packed agenda. Our Governing Board welcomed back returning, long-time public safety advocate Dr. David Boyd, Director, Office for Interoperability and Compatibility. Our Governing Board also presented David Buchanan, Chair, Spectrum Management Committee, with a plaque recognizing his outstanding work on a number of complicated issues on behalf of public safety communications, and recognized Gary Pasicznyk's work as Chair on the LightSquared/GPS interference issue and Charley Bryson's service to public safety through well-received daily outreach news blasts to NPSTC listserv subscribers.

**Dave Buchanan [L] thanks Ralph Haller [R] for NPSTC's recognition of his work**

NPSTC welcomed three new Governing Board members and alternates: Terry LaValley, representing the National Association of State Technology Directors (NASTD); Gary McCarraher, Alternate, International Association of Fire Chiefs (IAFC); and John Theimer, National Association of State Foresters (NASF). On behalf of our Governing Board, I would also like to thank former members, Michael Hutton, NASF; William Nelson, IAFC; and Wayne Gallant, NASTD, for their service to public safety telecommunications.

In other actions, the Governing Board was pleased to issue an invitation to Public Safety Communications Europe (PSCE) to apply to join NPSTC as a liaison member. PSCE, a European Union (EU)-funded non-profit organization, contacted NPSTC with an interest in joining the organization. PSCE's mission is to foster, through consensus building, excellence in the development and use of public safety communications and information management systems, to improve the provision of public safety services and the safety of the citizens of Europe and the rest of the world.

Two new issues arose at the meeting and NPSTC will be reaching out to educate public safety on these subjects:

- Interoperability problems are surfacing nationwide with new non-ANSI standardized digital radio platforms being introduced on Part 90 public safety radio spectrum. With the exception of the 700/800 MHz bands where specific technologies are required on interoperability channels, there are no restrictions on the lower bands. Day-to-day interoperability on agency channels is destroyed by incompatible technologies. A number of manufacturers have introduced proprietary digital systems causing interoperability and operability problems. NPSTC will develop a white paper on emerging digital radio technologies.
- After TV clearing from the 700 MHz band, the states were given 5 years to begin building out 700 MHz narrowband systems. The original rule was tied to 5 years after TV clearing; however, TV clearing occurred later than the original date specified. In July 2011, the FCC issued a clarification on the buildout dates, revising the date to June 13, 2014, but the criteria for demonstrating state buildout to the FCC are not clear. The state has to provide or be prepared to provide substantial service to one-third of the state's population or territory. Substantial service is vaguely defined as “sound, favorable, and substantially above a mediocre level of service. NPSTC volunteers are researching how to demonstrate the buildout requirement has been met.

Please join us in person or by teleconference at NPSTC's quarterly Committee meetings on the following dates:

- November 28, 2011, Call-In Meeting
- February 24, 2012, Las Vegas, NV
- June 5–6, 2012, Washington, D.C. [NPSTC's 15 year anniversary]
- September 10–11, 2012, Location TBD

## Well-Deserved Congratulations to Marilyn Ward, 2011 DeMello Award Winner

"Marilyn Ward can be described as the glue that keeps the public safety community together," says Ralph Haller, NPSTC's Chair. "She helped found NPSTC and chaired the organization for several years. Her untiring devotion to improvement of public safety communications has resulted in numerous rule changes at the FCC, all favorable to public safety. She stays on top of all issues affecting public safety communications and makes sure that NPSTC reacts as needed. Dick DeMello was also a founder of NPSTC and worked incessantly in the interest of public safety," says Haller. "Marilyn has all his positive traits and flawlessly carries on his ideals."

The first winner of the DeMello Award, Chief Harlin McEwen, will make the presentation to Ms. Ward at the Radio Club of America 102nd Annual Awards Banquet, celebrated this year at the Texas Motor Speedway in Dallas, Texas. "Marilyn Ward has been an untiring champion of improving public safety communications for many years," Chief McEwen says. "As the first Chair of NPSTC, she was able to bring together representatives of organizations who traditionally did not work well with each other. We have waited far too long to recognize the person mainly responsible for the many years of success we have seen at NPSTC. I am pleased that I will be able to present this award to my longtime friend Marilyn Ward."

"Marilyn is a remarkable professional in a public safety world where excellence is the standard," says Chief Alan Caldwell, last year's DeMello award winner. "Those of us who know her and work with her have great admiration, not just for her technical abilities, but for her savvy in dealing with thorny people issues. She is gracious, thoughtful and a joy to work with. Marilyn is the one we want on our team."

As an advocate of public safety telecommunicatios progress for almost 40 years, Marilyn Ward has dedicated her life's work to the advancement of interoperability among emergency responders. Ms. Ward currently serves as the Executive Director of the National Public Safety Telecommunications Council (NPSTC) — a collaborative federation of 15 organizations, whose mission is to improve public safety communications and interoperability through collaborative leadership. "Marilyn's middle name is 'consensus builder,'" says Tom Sorley, Deputy Director of Radio Communication Services in Houston, Texas, and Chair of NPSTC's Technology Committee. "When NPSTC was formed almost 15 years ago, there was some friction between several of the groups. Bringing them all to the table required a great deal of flexibility and diplomacy. Marilyn's straightforward manner and consensus-building skills were instrumental in helping to find common ground."

Marilyn Ward joined the Florida Highway Patrol when she was 20 years old. She has served public safety as a dispatcher, police officer, manager of Communications for the city of Orlando, and as a public safety telecommunications administrator.

Ms. Ward served as the Orange County, Florida, Communications Manager until March 2005. Appointed September 1999, Ms. Ward served in Orange County, Florida, managing 9-1-1, Radio Services, and Government Information. She was the project manager for the 3-1-1 Project and is the Chair of the Governor's Statewide Regional Domestic Security Task Force Interoperability Committee. "After 9/11, Florida's Governor appointed a domestic security task force and Marilyn was named the Statewide Communications Committee Chair," says Sorley. "She developed a network of regional chairs and developed and implemented many projects to improve interoperability throughout Florida."

Ms. Ward is also a member of the Radio Club of America, and serves on their Board, and former president of the Association of Public Safety Communications Officials - International. She serves on the Department of Homeland Security's SAFECOM Executive Committee. Former DeMello winner, Charles Werner, Fire Chief, Charlottesville, Virginia, says, "Marilyn Ward has been a leader in public safety communications in every aspect throughout her entire career; especially while serving on SAFECOM. Whenever there is a public safety communications issue, you will find Marilyn hard at work to resolve it. Whenever there is a monumental communications breakthrough, Marilyn is at the center. Clearly, public safety communications would not be what it is today without Marilyn's contributions. Marilyn is a visionary leader, a collaborator, a mentor, and a person I am proud to call friend."

"Marilyn's determination to reach consensus on communication issues among public safety entities is unparalleled. She is a determined, inspirational leader who has been the impetus for many of the advances made in our field in the last 20 years. She carries this off with a grace and genuineness that are unequaled," says Sorley. "We are lucky to have her on our side."

**Award Named to Honor DeMello's Achievements**

Beginning in 2005, NPSTC has presented an annual award to one public safety communications person who has demonstrated the highest levels of personal and professional conduct and performance in the local, state, and national public safety communications arena. The Richard DeMello award was named to honor the achievements of DeMello, one of the founding fathers of NPSTC.

**DeMello Award Sponsors**

Thanks to DeMello Award Sponsors for their support: Silver Contributors: The Forestry Conservation Communications Association (FCCA), and individual, Gregory Ballentine. NPSTC thanks Bronze Contributor, William Brownlow, and Certificate Contributors: Rich Reichler and Vincent Stile.

**Radio Club of America**

RCA was formed by a small group of dedicated radio amateurs and experimenters over a century ago. The Radio Club of America counted among its membership the very best in the radio communications industry, including the pioneers who shaped the industry.

## Concepts on Information Sharing and Interoperability

*by John Contestabile*

*[courtesy Johns Hopkins Applied Physics Lab] 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.*

---

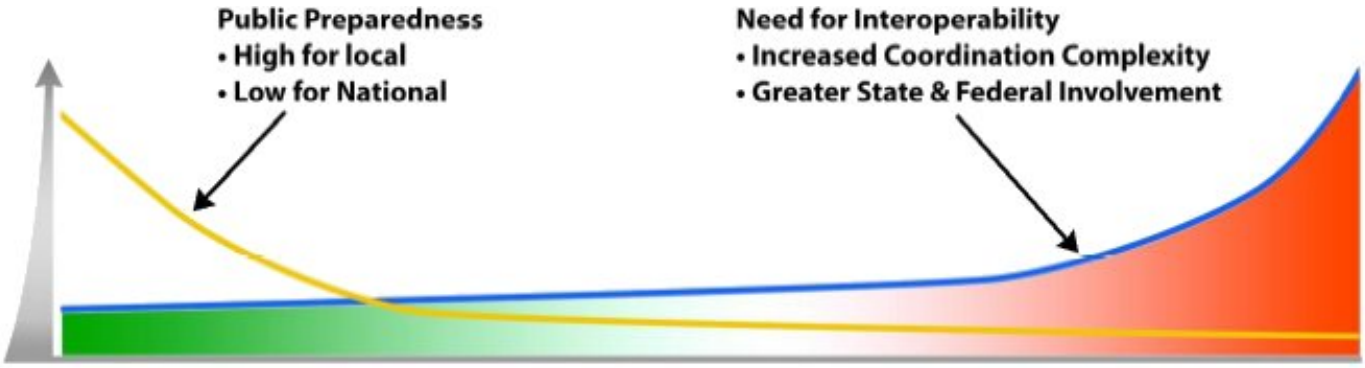
This paper addresses a conceptual framework for sharing information across jurisdictions, agencies and public safety disciplines. It was developed as part of the NCR jurisdictions (i.e. Maryland, Virginia, and the District of Columbia) interoperable communications programs. The paper explores why information 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 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**

**INCIDENT SCALE/PUBLIC PREPAREDNESS**




| Classification | LOCAL | REGIONAL | STATE | NATIONAL |
|---|---|---|---|---|
| Examples | • Minor Traffic Incidents<br>• Vehicle Fires<br>• Minor Train/ Bus Accidents<br>• Accidents W/ Injuries but no Fatalities | • Train Derailment<br>• Major Bus/Rail Transit Accidents<br>• Major Truck Accidents<br>• Multi-vehicle Crashes<br>• Hazmat Spills<br>• Injuries & Fatalities | • Train Crashes<br>• Airplain Crashes<br>• Hazmat Incidents<br>• Multi-vehicle Accidents<br>• Tunnel Fires<br>• Multiple Injuries & Fatalities<br>• Port/Airport Incidents<br>• Large Building Fire or Explosion<br>• Industrial Incidents<br>• Major Tunnel/ Bridge Closure | • Terrorist Attack/WMD<br>• Floods, Blizzards, Tornadoes<br>• Transportation Infrastructure Collapse<br>• Extended Power/Water Outage<br>• Riots<br>• 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 fewer 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.

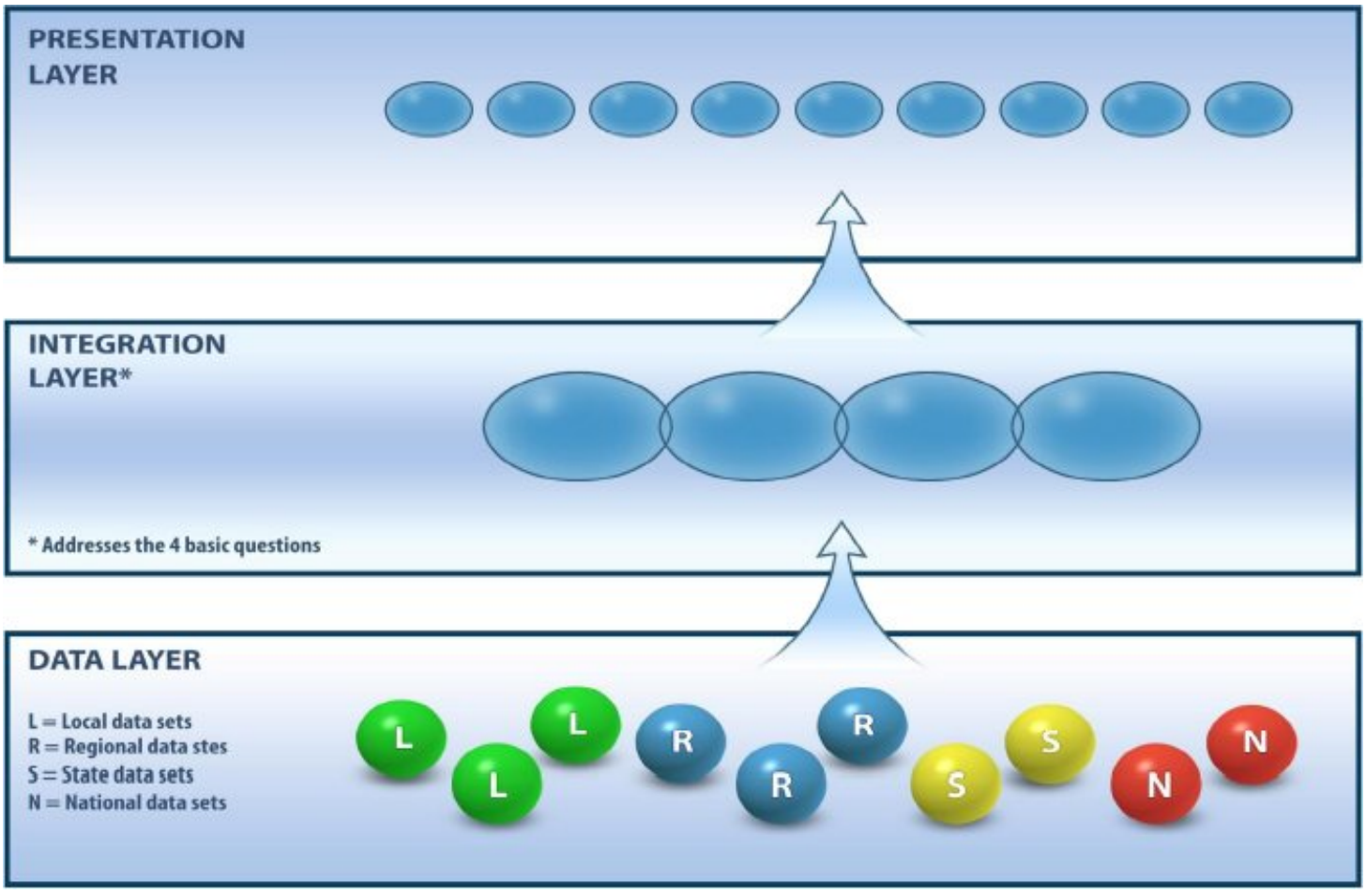
One method of improving data sharing would be to create interfaces between all the disparate systems at the data layer but, for some of the reasons noted above, this is problematic. Additionally, if one were to provide for interoperability at this layer, it would result in a multitude of "one off" connections. 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:




**What Tools should be Provided in the Integration layer?**

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:*

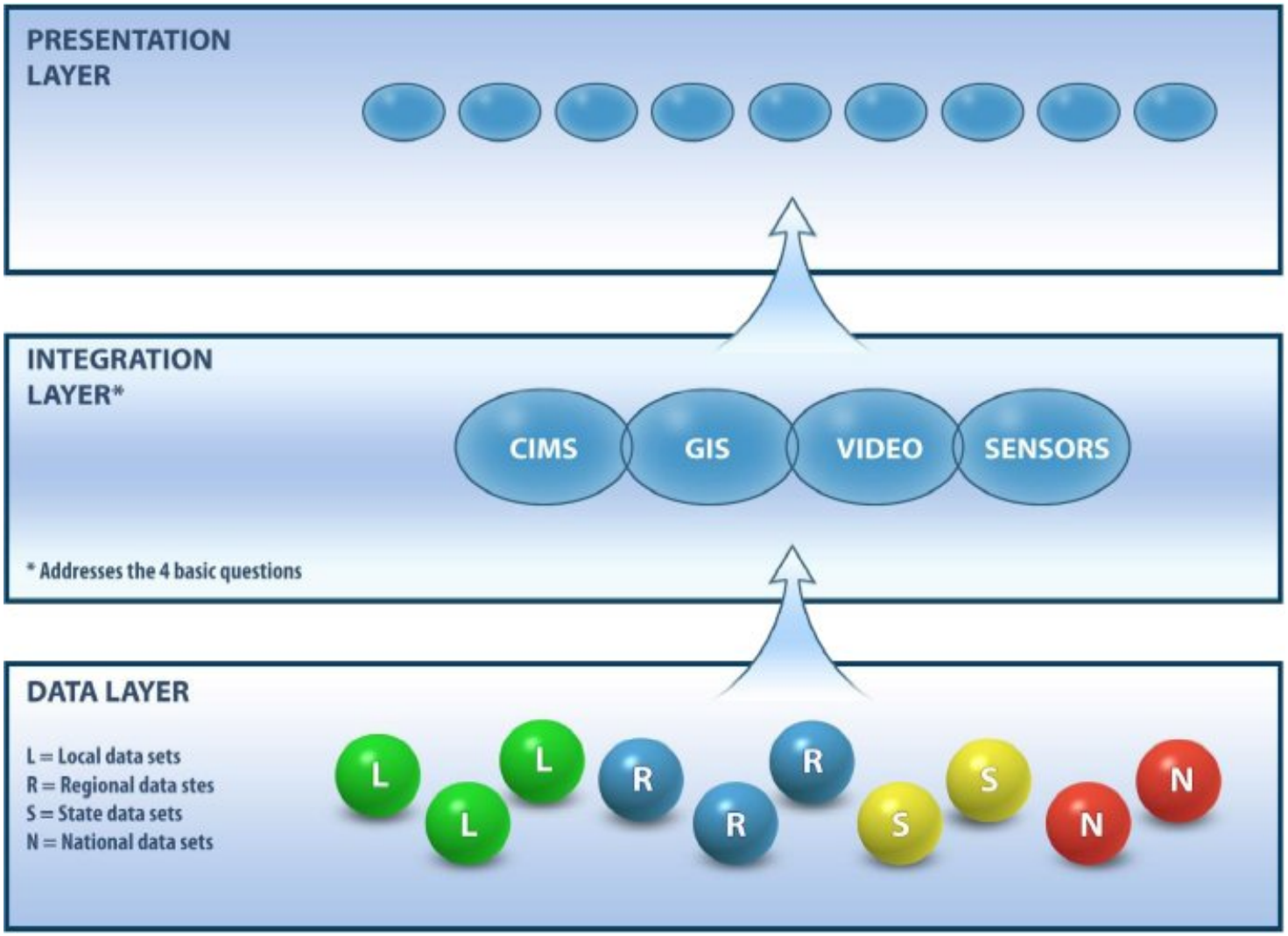
1. Where is it?
2. Can we talk about it?
3. What do we know about it?
4. Can we see it?

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.

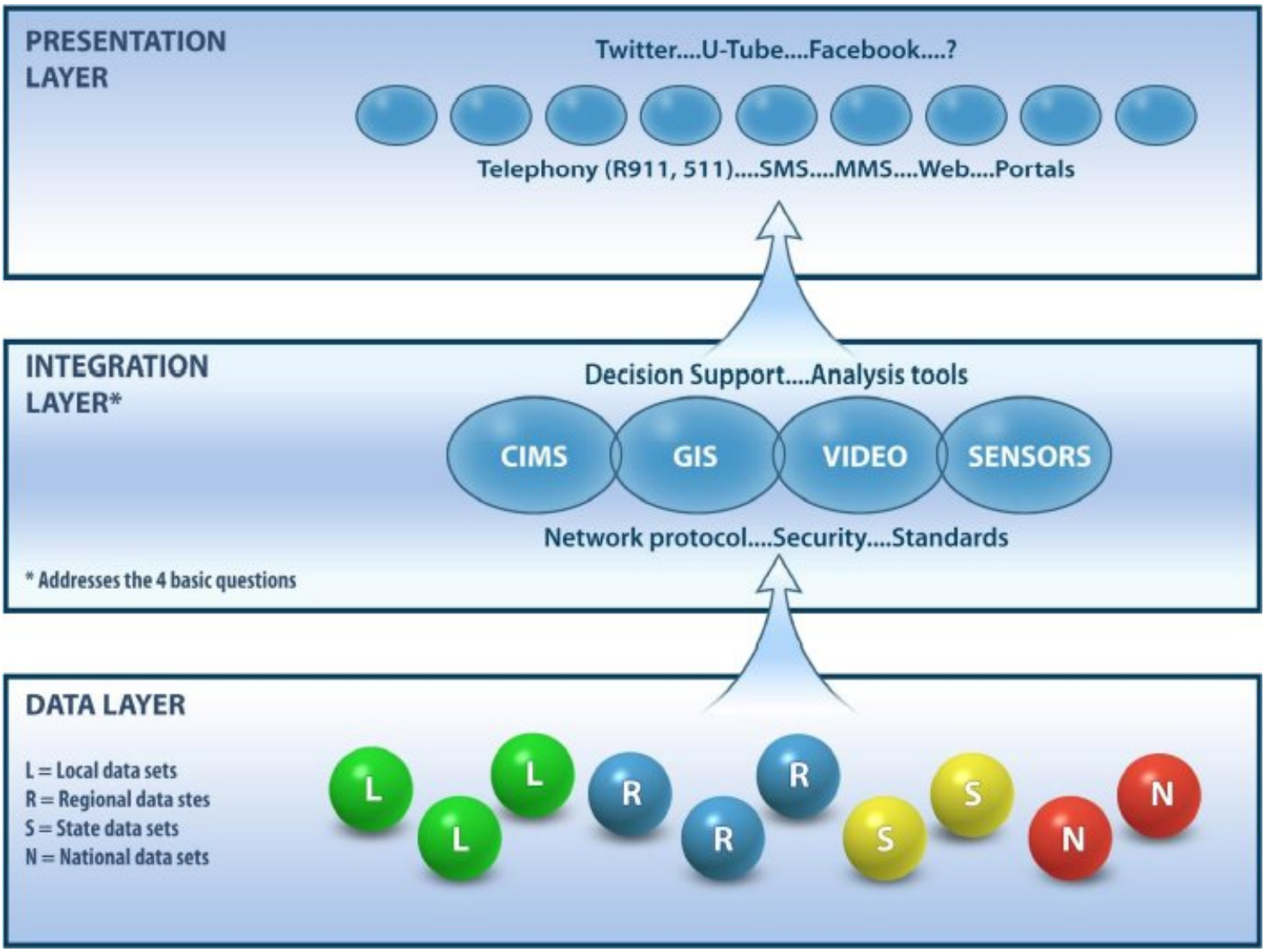
Revisiting the Conceptual Interoperability Schema graphic, the integration layer tools could be labeled as noted below.



**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.

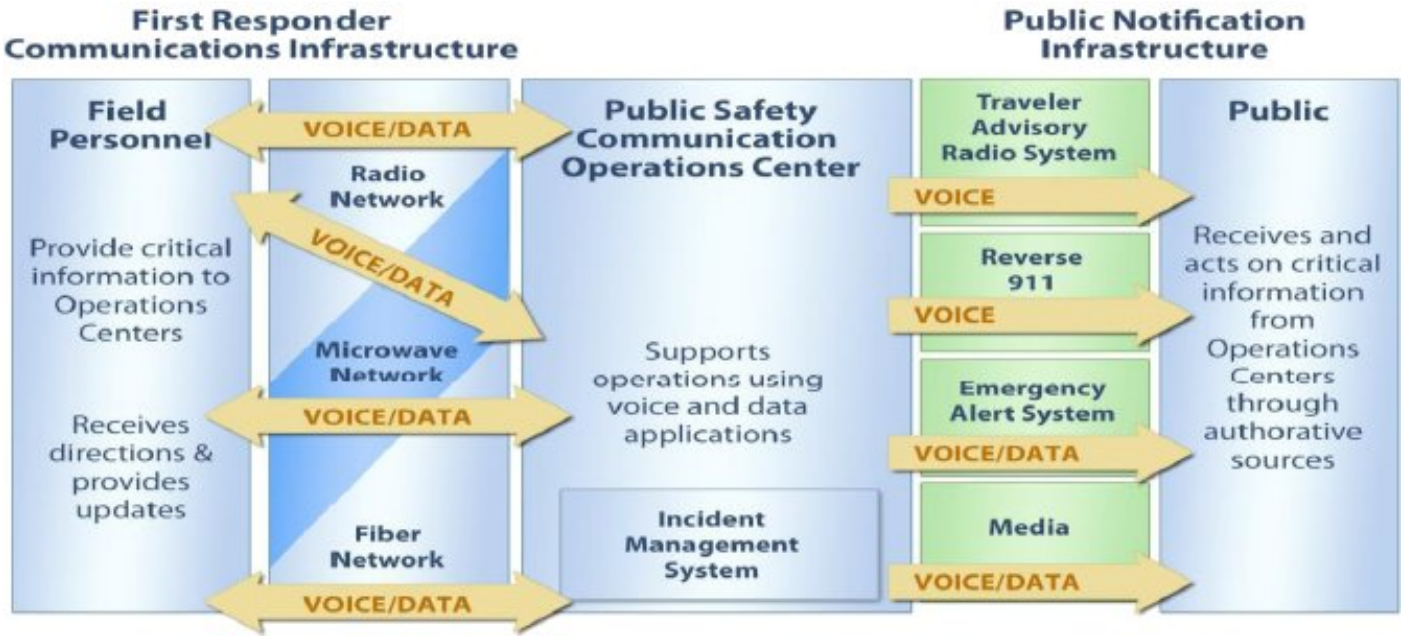



**Operational Model**

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**




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]

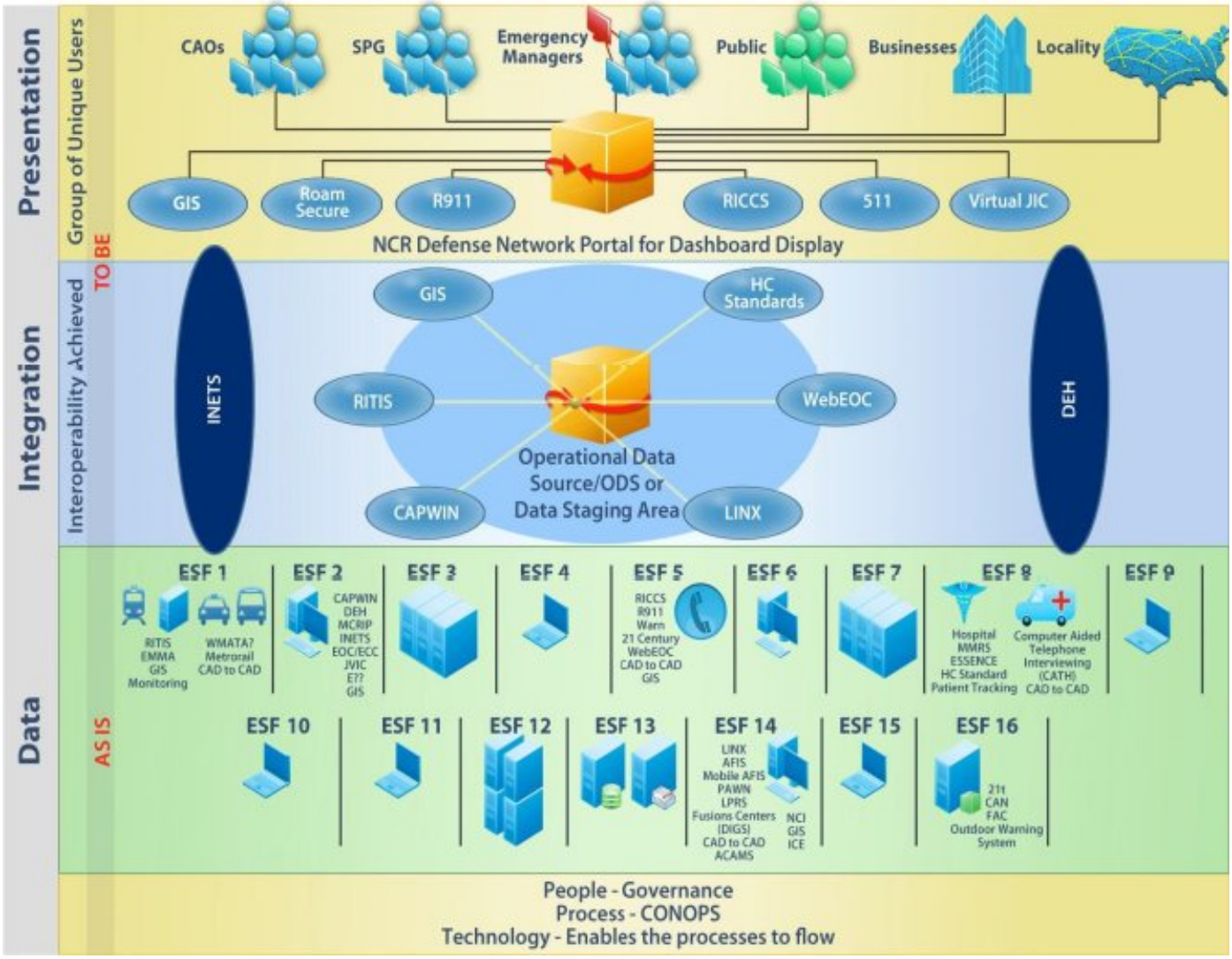
These varied methods of information distribution via automated means would speed the dissemination of authoritative information to the public during incidents when timely and accurate information sharing is critical.

**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 invested 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.



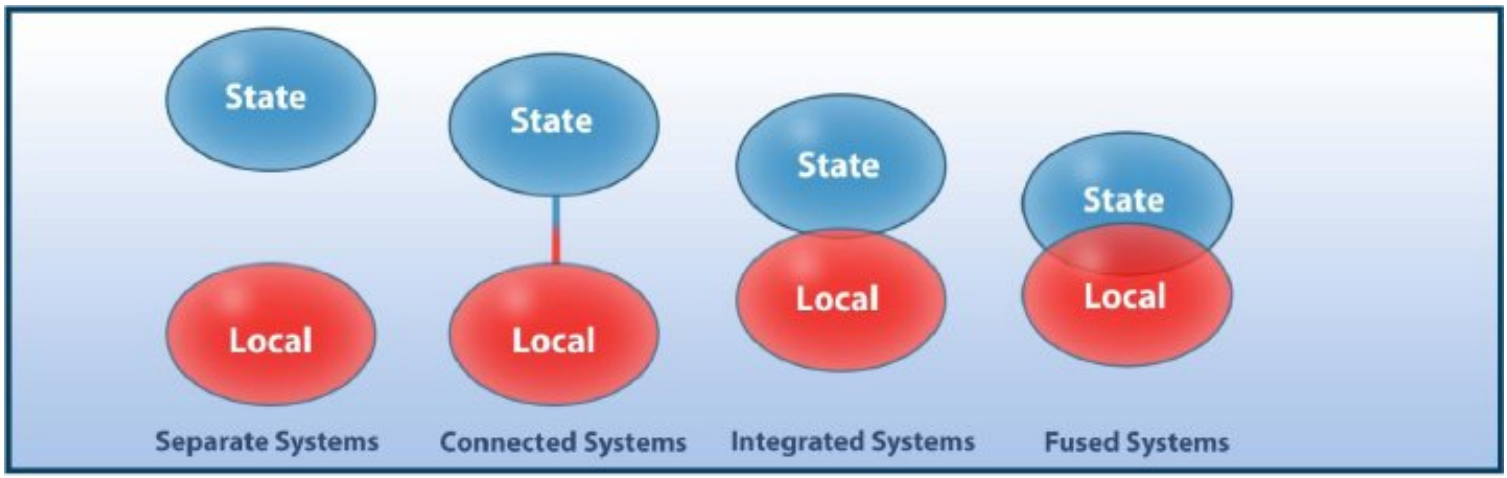

**What are the Benefits and Challenges?**

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 to 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.





**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

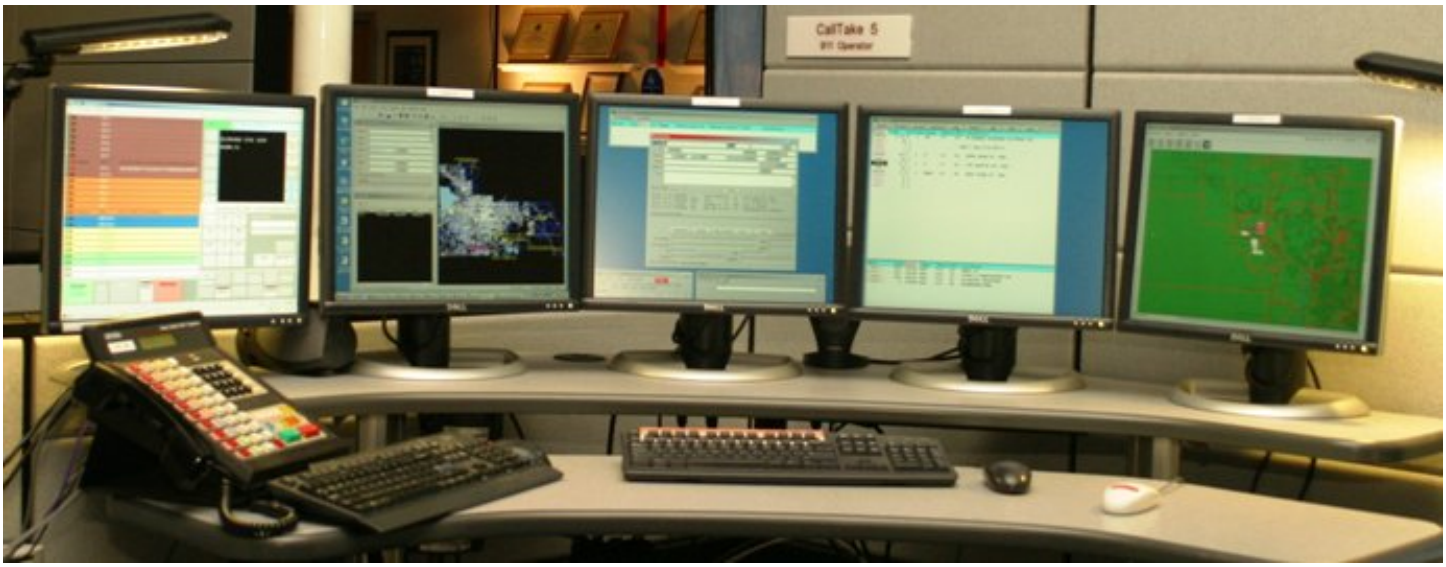
tools are also useful in this layer to bring key information to the decision makers attention.

- 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.

## Next Generation 911 What's Next Forum

**Prepared by the Transportation Safety Advancement Group (TSAG)**
***Report from Law Enforcement, Fire-Rescue, Emergency Medical Services, and Transportation Operations Stakeholder Panel***

When a major traffic accident occurs on the highway, local 911 centers receive increased numbers of calls alerting them of the accident. When Next Generation 911 (NG911) is widely available, how will the PSAPs manage the volume of text messages they are sure to receive?



The NG911 What's Next Forum, convened by the Transportation Safety Advancement Group (TSAG) at the request of the U.S. Department of Transportation (USDOT), Intelligent Transportation Systems Joint Program Office (JPO), examined that issue through panels of law enforcement, fire/rescue, emergency medical services, and transportation professionals at a forum that asked questions about the changes NG911 will create and how to address them. The project is co-managed by the JPO and the National 911 Program at the National Highway Traffic Safety Administration (NHTSA).

The Report covers the initial recommendations of subject matter experts in law enforcement, fire/rescue, emergency medical services (EMS), and transportation operations on the types of information that could be transmitted to them as end users of the forthcoming NG911 system. "To date, much of the discussion about NG911 has taken place in the technical arena. This report is intended to aid that effort by providing insight into the cultural, organizational, and operational environments in which NG911 will be implemented."

In September 2010, the What's Next Forum met in Washington, D.C., hosting a group of subject matter experts in four emergency responder professions, 911 technical experts, and public safety experts. Panelists were asked to identify major challenges facing their professions and to discuss ways in which NG911 could help them fulfill their missions as emergency

responders.

The original 911 system, introduced in 1968, was based on wired telephones connected by landlines. Since then the original system has been updated in many locations to include such features as automatic location information and the capability to route wireless calls, the report says. Devices and technologies are growing faster than the legacy 911 system's ability to keep up. The time has come to update the 911 infrastructure to enable the transmission of digital information (e.g., photographs, video, etc.) from callers to the 911 center, and on to emergency responders. Next Generation 911 is a system of 911 services and databases that run on an Emergency Services Internet Protocol (IP) Network (ESInet). The ESINet has been designed as an emergency services network, not just a 911 network. This network can allow automatic and advanced sharing of digital data among all public safety responders, public safety answering points (PSAPs), emergency management, traffic operations, and other entities.

**Need for Standards**

The panel members agreed that standards and interoperability are among the most important considerations for a NG911 environment. The report states, "Standards need to be defined in advance of development to ensure seamless interface with legacy systems and to transfer data to other PSAPs." "Interoperability" is a multifaceted concept, with different levels of meaning even within a discipline such as law enforcement.

It is often applied in a narrow sense, describing the ability of radio systems to communicate with each other, either within an agency or between different agencies. As a larger issue, interoperability suggests a state in which law enforcement agencies are capable of communicating with and working with departments in neighboring jurisdictions and with outside agencies such as fire, EMS, public works, towing, hospitals, transportation, state and federal agencies, etc.

**Managing Information and Avoiding Overload**

NG911 presents the likelihood of increased information flowing to field responders. Best practices for "information management" call for determining what data is to be sent, when, and to whom, and the NG911 system should support this as an agency-level decision.

Equally important, the report says, particularly for law enforcement agencies that operate or oversee PSAPs, is the need to properly manage information flow and avoid overload in the PSAP itself. Call-takers who are overwhelmed with information, or who lack direction or training on prioritizing data or making decisions when different data sources conflict, may require assistance from technology to "make sense of the data."

It is anticipated that NG911 will lower barriers to communication, possibly leading to a dramatic increase in the volume of incoming data (this is because the ease of sending a text or e-mail, together with the perception of anonymity, could make it more likely that people will use 911). At the same time, this increase in data volume could come with a corresponding decrease in the reliability or completeness of that data, especially if it comes from members of the public.

To prevent law enforcement and PSAPs from being paralyzed by information overload, technical solutions will be necessary to help analyze, route, prioritize, confirm, and otherwise act on incoming data. The law enforcement community would also benefit from a collaborative effort to draft policies and sample standard operating procedures that pertain to the above.

**Common Concerns**

The report lists these non-prioritized concerns across the participating public safety groups:

1. **Safety is a top concern.** Enhancing safety for responders and citizens should be a key consideration in the development of NG911. Priority should be given to developing data, applications, and capabilities that enhance the ability of emergency responders to operate safely, as well as their ability to carry out their missions to enhance public safety.
2. **Response-related information should be prioritized.** Although it is anticipated that further discussion and formal processes will be necessary to prioritize the data that is communicated to field responders via the NG911 system, the panels suggest that a high priority should be placed on data and capabilities that relate to response — that is, getting the right responders to the correct location in the least amount of time appropriate for the situation.
3. **Overload should be avoided.** Filter data and deliver necessary information at a time and in a manner that avoids "information overload" for responders.

4. **Interoperability is a key consideration.** All four panels noted the importance of interoperability, and several panelists suggested that NG911 carries the potential to introduce complexity in interoperable communications.
5. **Importance of uniform standards underscored.** NG911 technical standards and open architecture protocols developed in parallel with a national NG911 deployment plan are extremely important.
6. **NG911 should be considered a matter of national importance for emergency responder groups.** All the panels reported there has been little publicized national activity within their professional disciplines related to NG911.
7. **Rural agencies' needs must be considered.** NG911 may offer significant potential benefits to residents and emergency responders in rural areas, where emergency responders typically operate with fewer resources, limited personnel, extended response times, greater distances to hospitals, and other special challenges.
8. **Consideration must be paid to the needs of people with hearing disabilities.** People with hearing disabilities have been enthusiastic adopters of text messaging, instant messaging, sign language-compatible video chat, and related technologies for their daily personal and business communications. These newer enabling technologies are typically not compatible with the current 911 system, and callers using them must rely on an intermediary to contact help in an emergency.
9. **Stakeholder education is essential.** Without concerted education/outreach efforts directed at their professions, NG911 will likely continue to be viewed narrowly by many in their professions, as a primarily technical topic, with a perceived scope that begins with callers and ends at the PSAP.
10. **A clear process for future collaboration will build support and buy-in from stakeholder groups.** Stakeholder groups expressed a commitment to ongoing participation in collaborative steps as NG911 is developed.
11. **Emergency responder agencies will likely require assistance with costs.** Emergency responder agencies are extremely concerned about the costs associated with technology, training, and other expenses of transitioning to and operating in an NG911 environment.

*The Transportation Safety Advancement Group (TSAG) is a multidisciplinary assembly of professionals sharing a common interest in promoting technology for public safety. Members represent emergency response and public safety domains including fire and rescue, emergency communications, emergency medical services, law enforcement, transportation operations, emergency management, technology and telematics, and academic and research.*

*TSAG serves as a forum for the review of technologies for the emergency response interests in transportation-related public safety and provides input to the USDOT, ITS Joint Program Office. TSAG volunteer members are dedicated to enhancing both traveler and responder safety on the nation's transportation networks through the application of advanced technologies in emergency communications and response, and the promotion of interdisciplinary and interagency coordination. www.tsag-its.org.*

***Dia Gainor, Chair***
*Transportation Safety Advancement Group, dgainor@tsag-its.org*

## Science and Technology Directorate Wins Two Awards for Cyber Security

*Posted by Doug Maughan, Director, Cyber Security Division, DHS Science & Technology Directorate*

Throughout Cybersecurity Awareness Month, we have discussed the importance of making the Internet safer and more secure. This is a shared responsibility, and each of us has a role to play. Emerging cyber threats require the engagement of the entire society — from government and law enforcement to the private sector and most importantly, members of the public. Last week, the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) received two awards for work in strengthening our nation's cybersecurity posture.

We received a National Cybersecurity Innovation Award at the Sans Institute's Second Annual National Cybersecurity Innovation Conference for our Domain Name System Security Extensions (DNSSEC) project, which protects the public by ensuring that websites visited are the real deal and not imposters. Phony websites steal users' log-in names, passwords, and even money, from thousands of innocent Internet users every year. S&T's Cyber Security Division (CSD) was recognized for its innovation in promoting research that "pays off" by focusing on work that can result in real products and real risk reduction. Moreover, the award noted that the CSD's approach has forced the R&D community to think beyond the theoretical to consider a more practical horizon.

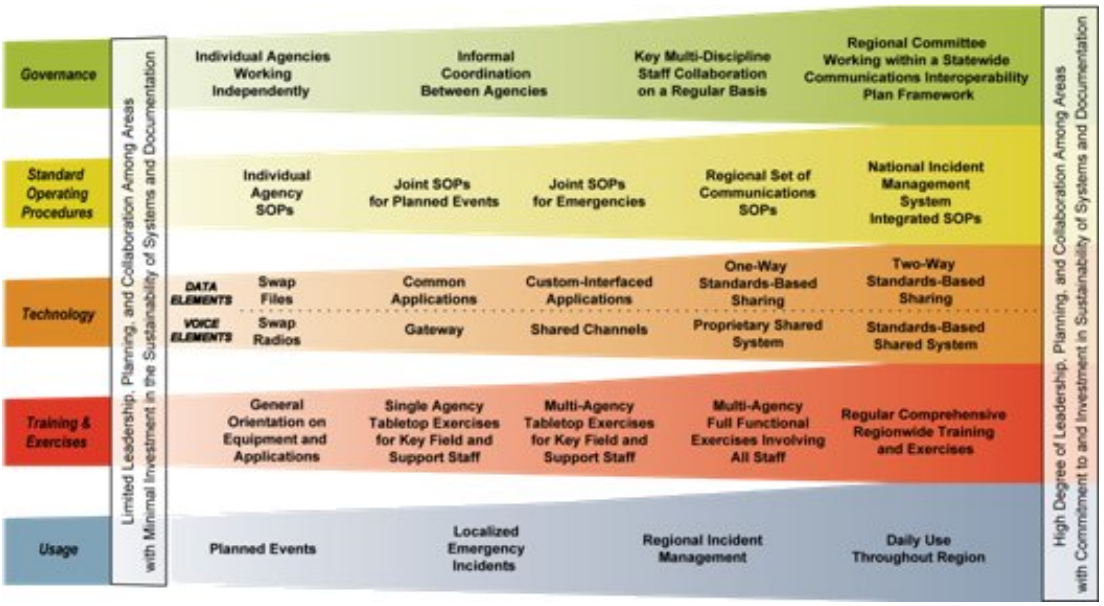
DHS S&T also received the Open Source for America (OSFA) 2011 Government Deployment Open Source Award for the Homeland Open Security Technology (HOST) project, which brings together technology leaders from across government and developing advanced open source security solutions that address their prioritized gaps. This award recognizes projects and people that educate decision makers in the federal government about the advantages of using free and open-source software and encourage federal agencies to give equal priority to procuring free and open-source software in all of their procurement decisions. The development of the open source intrusion detection system, Suricata, was sponsored through this project and is now being sustainably maintained by industry through a non-profit foundation.

The DHS Science & Technology Directorate is leading efforts to develop and deploy more secure internet protocols that protect consumers and industry internet users. As evidenced by these awards, the Department is making significant strides to enhance the security of the nation's critical physical infrastructure as well as its cyber infrastructure and networks

Source: http://blog.dhs.gov/2011/10/science-and-technology-directorate-wins.html

## OEC Showcases Successful Implementation of the Interoperability Continuum

To highlight advancements made by stakeholders, OEC published five case studies in September 2011 that align with the SAFECOM Interoperability Continuum. Through these case studies, OEC is highlighting examples from various jurisdictions across the nation so that others will be able to understand the complexities of interoperability and determine how the innovative solutions included in the studies might help them overcome their own barriers. The case studies include:




Governance — New York City Interagency Communications Committee as an example of how jurisdictions are demonstrating the capability of managing a regional committee working within a multi-state framework.

Standard Operating Procedures — Minnesota Allied Radio Matrix for Emergency Response (ARMER) as an example of comprehensive interoperability achieved through procedures and protocols governing response designed prior to an incident.

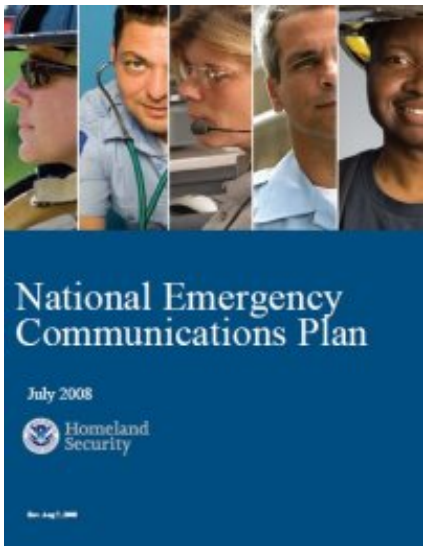
Technology — Delaware Statewide Emergency Communications System as an example of a standards-based, regionally-shared system that supports more than 14,000 subscribers from 247 different local, State, Federal, and non-governmental agencies, processing more than 115,000 interoperable communications calls on a routine day.

Training and Exercises — Washington State Integrated Interoperable Communications Plan, developed in preparation for the 2010 Olympic Games, as an example of an interagency communications plan adapted into a two-day curriculum enabling students to apply their new communications skills through a series of tabletop exercises.

Usage — Louisiana Wireless Information Network (LWIN), developed as part of the recovery efforts of Hurricane Katrina, as an example of a multijurisdictional system that provided vital support to local, State, and Federal responders during responses to Hurricane Gustav and the Deepwater Horizon oil spill.

These case studies highlight just a few examples of the tremendous progress made in the field of emergency communications since that tragic day in 2001. While much has been accomplished towards achieving nationwide interoperability in the last 10 years, there is still work to be done. OEC plans to continue publishing case studies in the future. If you are interested in highlighting a project or success in your jurisdiction, please contact OEC@dhs.gov.

## NECP Update from Office of Emergency Communications




As you all know, one of the key interoperability initiatives for the Office of Emergency Communications (OEC) is the National Emergency Communications Plan (NECP). The NECP serves as the first national strategy for interoperability and provides a roadmap for public safety and government officials to make measurable improvements in emergency communications.

Implementation of the NECP has been a key driver behind much of our progress in improving interoperability. More than 85 percent of the NECP milestones have been achieved to date, and progress is evident in all of the NECP priority areas, such as governance, training, and coordination. In addition to the objectives, milestones, and benchmarks in the NECP, there has been significant progress in achieving the performance-based goals contained in the Plan.

**NECP Goal 1 Achieved**

Goal 1 of the NECP required *"By 2010, 90 percent of all high-risk urban areas designated within the Urban Area Security Initiative (UASI) are able to demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions and agencies".*

To measure the progress towards achieving Goal 1, OEC worked with the nation's UASI regions to assess their ability to demonstrate response-level emergency communications during planned events that included large public gatherings and required participation from multiple public safety agencies and jurisdictions. Observation teams, consisting of state and local peer observers and OEC staff, used criteria developed by experienced public safety and communications professionals in the field to measure the urban area's communications performance. The criteria focused on key elements of response-level emergency communications, such as how well leadership levels communicated with each other, managed resources, and made decisions. The observation teams also observed whether policies and procedures for communications were used successfully during the event.

Following each Goal 1 demonstration, observation teams completed after-action reports and improvement plans for each event based on the established criteria, which were then provided to each urban area point of contact. Based on the NECP Goal 1 assessments, OEC concluded that all participating UASI regions were, to varying degrees, able to demonstrate response-level emergency communications and have instituted the necessary capabilities to achieve interoperability among multiple agencies and jurisdictions during large-scale planned events.

**NECP Goal 2 Assessment**

NECP Goal 2 requires *"By 2011, 75 percent of non-UASI jurisdictions are able to demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions and agencies".*

This goal focuses on the ability of non-UASI regions to demonstrate response-level communications in a multi-jurisdictional event. Currently, OEC is working with the states and territories to assess their counties' or county-level equivalents' ability to achieve this goal during exercises, real-world incidents, or planned events. The results of these assessments will provide public safety agencies with the performance and capability data necessary to build sound strategies for achieving and sustaining interoperability. These efforts will also assist OEC in better targeting grant and technical assistance support towards potential gaps identified in the assessment process.

**NECP Goal 3**

In the near future, OEC and our stakeholder partners will begin to assess the nation's ability to meet the requirement set by NECP Goal 3: *"By 2013, 75 percent of all jurisdictions are able to demonstrate response-level emergency communications within three hours, in the event of a significant incident as outlined in national planning scenarios."*

As part of the Goals 1 and 2 assessment process, OEC worked closely with representatives from the State and local community to establish performance measurement criteria that can provide on-going benefits to jurisdictions beyond just demonstrating the goal being assessed. OEC will use the same stakeholder-driven process to assess NECP Goal 3. As before, OEC will gather feedback and input from the public safety community on the best methodology for conducting the assessment and evaluation of Goal 3 and the data that will be gathered during the benchmarking process.

**Moving Forward**

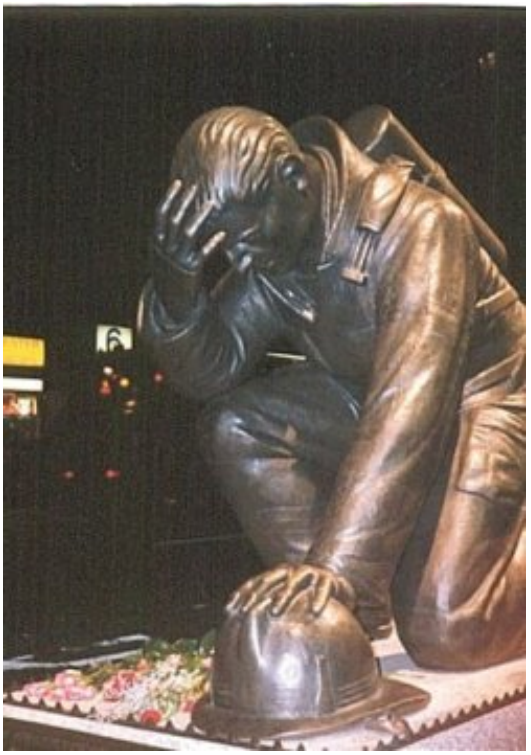
The completion of the NECP goal assessments marks an important step toward achieving national interoperability; however, work still remains. The results of these assessments will provide public safety with critical information to justify continued support of emergency communications and identify gaps to build a sound strategy for achieving and sustaining interoperability. Implementing interoperable emergency communications nationwide is a complex process, and OEC remains committed to improving emergency responders' communications capabilities and achieving the vision of the NECP.

## Remember the Past, Honor the Future - 9/11 Tribute

*Editor's Note: On September 11, 2011, NPSTC posted on our home page this tribute to public safety and to all who lost their lives.*

On this day we mourn the great tragedy of 9/11 and honor those who lost their lives in this tragedy and those who lost their lives trying to save others. From the Pentagon to Shanksville, Pennsylvania, to Ground Zero in New York City, and across the nation, we will raise the flag and share a moment of silence at 8:46 am EST, the moment the first plane hit the World Trade Center on September 11, 2001.

NPSTC also honors the dedicated Americans who have worked so diligently on many fronts to ensure our first responders can talk to each other in emergencies and every day to protect their lives and the lives and property of our citizens. Their conscientious efforts to improve collaboration and planning, to exercise, to make sure technologies are interoperable, and to acquire adequate spectrum for interference-free communications have greatly improved communications and the safety of our nation.



September 11, 2001, was a day of unprecedented shock and suffering in the history of the United States. The nation was unprepared. How did this happen, and how can we avoid such tragedy again? To answer these questions, the Congress and the President created the National Commission on Terrorist Attacks Upon the United States.

Americans responded vigorously to the challenges. The President authorized the new Department of Homeland Security (DHS) to protect and defend the nation's homeland. A bi-partisan 9/11 Commission Report made 41 recommendations for keeping our country safe. These recommendations were endorsed by almost every member of Congress. One of the findings of the 9/11 Commission was the absence of interoperable communications among public safety organizations was a problem of the highest order.

DHS stood up its Science & Technology Directorate, Office for Interoperability and Compatibility (OIC), and initiated the model guidelines of the SAFECOM program. Following Hurricane Katrina, Congress created the DHS Office of Emergency Communications (OEC) to enhance collaboration between federal, state, and local efforts and provide technical assistance to improve public safety communications.

9/11 raised awareness among public policymakers about the critical role emergency communications plays in incident response. These concerns prompted numerous national studies, plans, and strategies including OEC's National Emergency Communications Plan (NECP), a strategic roadmap for enhancing emergency communications. Interoperable communications have improved. Grant dollars have been dedicated to providing models and technical assistance to create good governance, collaboration, and cooperation between jurisdictions and agencies. OIC has supported promising technology and standards for public safety communications. Increased spectrum resources have also enhanced the ability of first responders to communicate, and, in the future, public safety will have access to the broadband resources the ordinary citizen enjoys.

## Regulatory Update

*by Bette Rinehart, Editorial Task Group Chair*

**Comment Sought on How To Facilitate Deployment of NG911**

The Federal Communications Commission (FCC) has released a Notice of Proposed Rulemaking (NPRM) asking for comment on the best ways to encourage deployment of technologies that will allow consumers to send texts as well as other non-voice information to Public Safety Answering Points (PSAPs) using 911. Because 4G communications devices are becoming more widely deployed, consumers have come to expect that they can communicate in non-voice ways with everyone, including contacting 911 during an emergency. Since the 911 system was designed to work with circuit switched landlines, wireless, non-voice communications are not possible using the legacy equipment.

In this NPRM, the FCC is specifically looking at ways to encourage the deployment of text-to-911 and asking whether an interim solution would provide sufficient benefit without being overly costly until full NG911 capability was possible. The FCC believes that providing a text-to-911 capability would not only be of benefit to persons with disabilities but would also be useful when a voice call was not possible either because of the danger of being overheard or because a network was unable to support voice due to network outages as the result of a natural disaster.

The Commission is also considering its role in facilitating and, if necessary, accelerating the deployment of NG911. The agency notes that NG911 deployment is unlikely to occur uniformly across the country and asks for comments on the best way to educate the public about capabilities, limitations and availability of NG911.

In response to experiences during the East Coast Earthquake and Hurricane Irene, the FCC also asked for comment on how and whether to prioritize calls to 911 over other calls during emergencies when wireless networks are often extremely congested causing call failure.

The News Release is available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-309746A1.doc

The text of the NPRM is available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-11-134A1.doc

The text of the White Paper on NG911 Costs is available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-309744A1.doc

---

**Scope of TETRA Waiver Clarified**

The FCC released an Order clarifying certain aspects of the waiver granted to the TETRA Association earlier this year allowing the certification and use of TETRA equipment under certain circumstances during the pendency of the larger rulemaking proceeding.

EWA, NPSTC, TIA, and Motorola had filed requests for clarification of certain aspects of the waiver including the ability to deploy TETRA on an existing system without receiving frequency coordination, deployment in 800 MHz bands where public safety continues to operate until rebanding is complete, and to which devices the prior certification exemption applied.

The Commission clarified its decision as follows:

- TETRA deployment in 862-869 MHz (former National Public Safety Planning Advisory Committee (NPSPAC)/current Enhanced Specialized Mobile Radio (ESMR) band) is not permitted in any NPSPAC Region until the FCC has issued a Public Notice announcing that rebanding is complete in that Region.
- Frequency coordination is not required if the only change to the technical parameters is "emission bandwidth" (e.g. a change from 20K0 to 21K0). Any change to the “emission type” requires frequency coordination (i.e., change from 20K0D1W to 21K0D1W allowed, but change from 20K0F3E to 21K0D1W requires coordination).
- TETRA equipment is required to meet the station identification requirements of 90.425 (station ID by either voice or Morse code).

- Low power TETRA equipment that was previously certified using 20K0 emission bandwidth may not be approved for full power operation unless a new equipment authorization application is filed and granted for 21K0 emission bandwidth.

Text of the Clarification Order is at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-11-1604A1.doc

---

**Public Testing of First TV White Space Database Announced**

The FCC has announced that a 45-day public trial of the first TV White Space database began on September 19. TV White Space is TV spectrum that is not being used for broadcast services. A fairly recent FCC decision permits the use of TV White Space by unlicensed devices if those devices first access a public database to determine what TV spectrum is available at that location. Testing of the database developed by Spectrum Bridge will help to ensure that it is functioning properly and accurately identifying TV channels available for use by unlicensed devices. Participants in the test are asked to report any inaccuracies or other issues with the database to Spectrum Bridge using a link on the trial's website.

The TV white space database is available at: http://whitespaces.spectrumbridge.com/Trial.aspx

The text of the Public Notice is available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-11-1534A1.doc

The text of the News Release is available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-309608A1.doc

---

**Deployable Aerial Communications Architecture White Paper**

From comments received in response to a Public Notice earlier this year, the FCC has written a White Paper on Deployable Aerial Communications Architecture (DACA). The White Paper outlines the types of DACA currently available, regulatory/tactical issues, and a set of next steps for the Public Safety Homeland Security Bureau (PSHSB).

After a natural disaster or other times when terrestrial communications systems are unavailable or overloaded, DACA could provide an interim infrastructure solution for public safety and commercial users until power or the physical site is restored. Hurricane Irene and the East Coast Earthquake were both cited as examples of the types of situation when communications are disrupted.

Among the types of DACA are:

- SUAV (small unmanned aerial vehicles); fly about 500' above ground, can stay airborne for several hours, can be used as a repeater or virtual cell tower and can support a single frequency band
- Weather Balloons; can act as repeaters, "gateways" to bridge different frequency bands within a system; can remain aloft for short periods of time and require frequent re-launching
- HALE (High altitude long distance unmanned vehicles); can be deployed at higher altitudes for longer periods and can support multiple frequency bands providing the potential for a deployment supporting a geographic region
- Deployable suitcase systems; can be placed in low-flying aircraft and used as repeaters
- Satellite technologies were mentioned as a critical component of most DACA connectivity

Next steps identified by the White Paper were:

- Initiate a Notice of Inquiry (NOI) by the end of the year to address FCC-related issues including operational procedures, frequency coordination, the role of DACA during disasters, costs/cost effectiveness, and licensing requirements.
- Host a workshop on DACA solutions and issues by the end of the year
- Share findings with FAA, FEMA and other federal partners to discuss possible pilot programs and implementation
- Determine issues that have international ramifications and work with the State Department and other federal agencies to determine the appropriate next steps

The text of the white Paper is available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-309742A1.doc

The text of the News Release is available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-309741A1.doc

---

**Deployable Aerial Communications Architecture (DACA) Workshop/Webinar Announced**

The Commission has already taken one of the next steps identified in the DACA White Paper by hosting a Workshop/Webinar on the topic on October 31, 2011. The Workshop consisted of three panels; the first discussed how DACA can ensure the viability of critical communications within the first few hours after a catastrophic event; the second focused on the types of DACA available and how they could be used; the final panel addressed technical issues including interference concerns.

---

**Lojack Vehicle Recovery System (VRS) Waiver Grants**

The LoJack Corporation had filed a request to waive the following requirements currently imposed on the operation of frequency 173.075 for Stolen Vehicle Recovery Systems:

- Permit activation of the tracking device by a portable device as well as a base station
- Permit non-police entities to activate the device
- Allow a duty cycle of 1000 milliseconds every 8 seconds for transmitting activation signals

LoJack is developing a wrist-watch-like device that is targeted to be worn by at-risk persons such as nursing home residents with dementia or Alzheimer's or children with disabilities. A handheld Portable Activation Tracker (PAT) is also being developed to activate and track the wristwatch devices over a limited geographic area. Permitting non-police persons to activate handheld PATs would allow nursing home personnel to quickly activate and begin searching for missing residents.

The waiver was put on Public Notice in January for comment on each aspect, particularly whether changing the duty cycle would impact TV Channel 7 reception or Federal use of 173.075.

This month, Lojack's waiver has been granted; non-police entities may activate the devices and the duty cycle has been amended as requested. The Commission on its own motion issued a declaratory ruling that the current rules permit activation by either mobile or portable units;

The Commission's decision indicated that allowing non-police entities to activate the tracking devices provides quicker response times and reduces the drain on police resources. Changing the duty cycle would not increase the potential for interference to Channel 7 or federal users of 173.075. New mobiles and portables operating pursuant to the waiver must remedy any interference caused to Channel 7 within 30 days of notification.The text of the decision is available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-11-1551A1.doc

---

**Lightsquared Must Continue to Test**

The FCC issued a Public Notice indicating that LightSquared must continue to test its proposed Ancillary Terrestrial Component (ATC) operations to identify and address potential interference to GPS systems those operations might cause. A technical group of over 100 participants including public safety, federal agencies and telecommunications companies tested GPS devices against LightSquared's proposed terrestrial devices and discovered the potential for harmful interference if LightSquared deployed as originally planned.

To address these concerns, LightSquared has proposed to limit its terrestrial operations to the lower 10 MHz of the band. Testing has shown that the interference potential is reduced but concerns remain for certain types of GPS receivers.

Therefore, additional testing is needed and until GPS interference concerns have been satisfied, LightSquared may not deploy ATC under its waiver. The text of the Public Notice is available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-11-1537A1.doc

---

**800 MHz News**

**Genesee County, NY vs Sprint Nextel:** The FCC has released a decision on a de novo review case between Sprint Nextel and Genesee County, New York. One of the issues of this case is that Genesee is arguing that because the proposed replacement frequencies for two of its system frequencies will, post-rebanding, be located within 1 MHz of ESMR operations, Sprint had not provided it with "comparable facilities." The underlying purpose of the entire rebanding proceeding was to separate ESMR and non-ESMR operations to the maximum extent possible and, in the Canadian 800 MHz decision, the Commission had directed that a 1 MHz separation between Public Safety and ESMR operation should be maintained.

Sprint argued, and the TA agreed, that because of the limited amount of spectrum available in the Canadian border region, a 1 MHz guard band between ESMR and non-ESMR operations cannot be established. Public Safety operations are fully protected from interference from ESMR operations so if interference occurs, Sprint must mitigate any interference that Genesee receives. Sprint also points out that Genesee's current operations are within 1 MHz of Sprint's operations; ergo comparable facilities.

The Commission agreed with Sprint and the TA's recommendations and ordered Genesee to produce a cost estimate within 30 days after which Genesee and Sprint Nextel must begin FRA negotiations.

The text of the decision is available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-11-1521A1.doc

---

**Rebanding Negotiations for Wave 4 Licensees in Mexican Border Extended:** The rebanding negotiation deadlines for 800 MHz incumbent licensees in the Mexican border have been extended as follows:

- January 3, 2012 – Negotiations end
- January 4, 2012 – Mediation begins
- February 15, 2012 – Application freeze ends

The text of the Public Notice is available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-11-1652A1.doc

## Message from the Public Safety Communications Research (PSCR) Program

*by Dereck Orr, Program Manager for Public Safety Communications*

*(courtesy National Institute of Standards and Technology (NIST's) Office of Law Enforcement Standards)*

Thank you for your continued participation in PSCR's 700 MHz Public Safety Broadband Demonstration Network project. The project continues to make progress, with over 35 Cooperative Research and Development Agreements (CRADAs) signed to date and more than 9 vendors installing and testing equipment in our labs. Phase 1 and Phase 2 Part 1 test plans are available on our website, Phase 2 Part 2 and Phase 3 will be available soon.

We were planning to host our third Stakeholders Meeting in November 2011, but due to end-of-year fiscal restrictions, we are now planning the meeting for the week of March 5, 2012. We are excited to have the opportunity to present test results, study item outcomes, and presentations from federal partners, industry leaders, and public safety representatives covering the most pressing

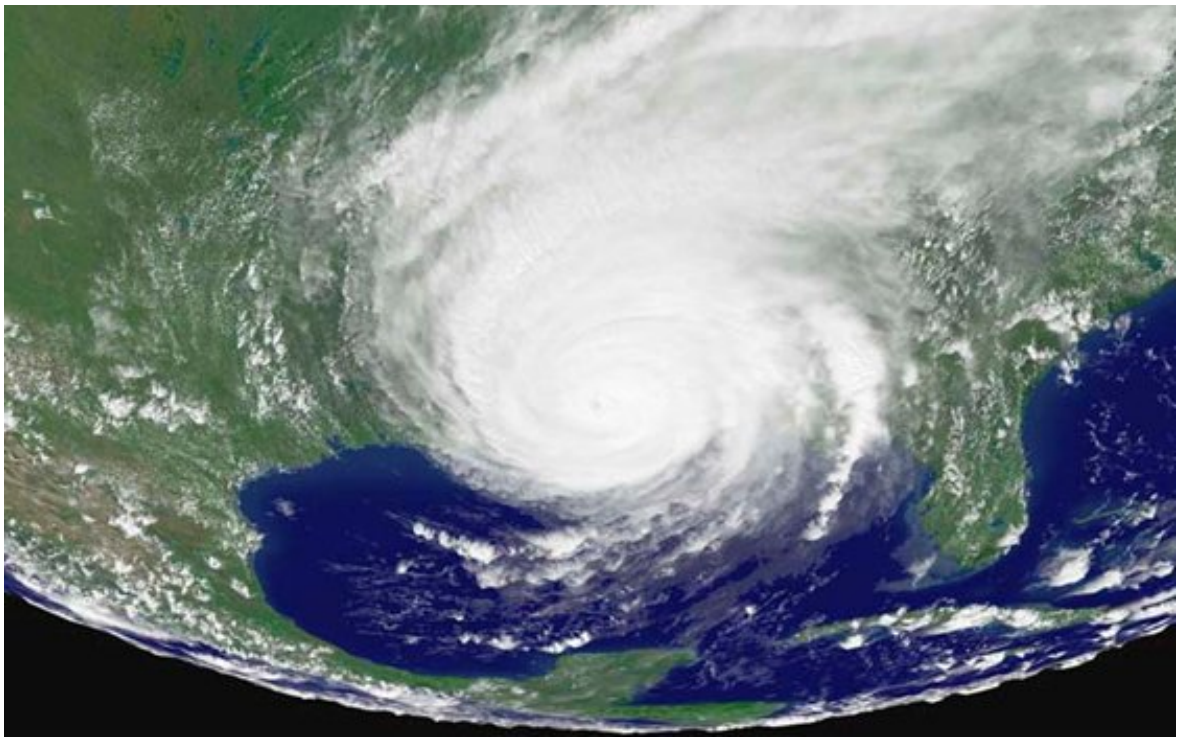
technical topics in public safety broadband.

In the meantime, we invite you to participate in a Network Identifiers Workshop Webinar that will present the outputs of PSCR's Network Identifiers Study Item research. Materials will be distributed to registered participants beforehand and there will be a significant portion of the agenda dedicated to Q&A. Comments gathered during this webinar will be used to inform PSCR's implementation of network identifiers on the PSCR Demonstration Network. This Webinar is tentatively scheduled for mid-January — details will be sent via the 700demo@its.bldrdoc.gov list serve as well as posted on our website, www.pscr.gov.

To update you on other activities, PSCR has been continuing our research on technical issues identified as priorities at the Winter 2010 Stakeholder Meeting, such as Roaming and Clearing, UE Testing, Priority/Quality of Service, and Network Identifiers. If you are interested in learning more about PSCR's research in these areas, please visit the Broadband project website at http://www.pscr.gov/projects/broadband/700mhz/700mhz.php. PSCR has also been actively participating in international standards bodies such as the 3rd Generation Partnership Project (3GPP), ATIS, and the Groupe Special Mobile Association (GSMA), as well as test forums such as PTCRB, the Network Vendors Interoperability Testing Forum (NVIOT), and the Multi Service Forum (MSF) to ensure that public safety's specific requirements are represented. Additionally, PSCR continues its involvement in NPSTC's Broadband Working Group, leading several task groups focused on gathering user requirements for features such as local control, voice, priority and quality of service, security, and multimedia emergency services.

Again, we appreciate your continued participation and look forward to sharing our progress with you in March 2012. Keep an eye out for formal announcement and registration information in the coming months. To learn more about the Demonstration Network and PSCR's other projects, please visit www.pscr.gov.

## ESF-2 Working Group Ready to Roll



The U.S. Department of Homeland Security's Federal Emergency Management Agency's (FEMA) Emergency Support Function-2 (ESF-2) has played a very important role providing communication services to disaster victims during Hurricanes Katrina and Rita. ESF-2 was responsible for the restoration/repair of telecommunications infrastructure for state, local, and private sector communications services. They also coordinated with telecommunications industries on restoration activities. Following the disaster, ESF-2 was deployed to assess the communications infrastructure in disaster-affected areas. The ESF-2 team also identified communications facilities, equipment and personnel located in and outside the disaster areas that could be available to support response and recovery efforts.

Last year, NPSTC stood up an ESF-2 Working Group to develop long-term processes and relationships between ESFs, FEMA, and the Regional Emergency Communications Coordination Working Groups (RECCWGs) that support emergency

communications from one jurisdiction to another.

"The mission of ESF-2 is to provide interoperable communications guidance across multiple jurisdictions, agencies, and disciplines," says Keith Victor, Working Group Chair. "ESF-2 serves as a primary operational level coordination mechanism to provide assistance in functional areas for regional communications. ESF-2 addresses the purpose, scope, policies, concept of operations, organization, actions, and other communications requirements for primary, support, and secondary public safety agencies."

Victor says he expects the Working Group to develop plans for bringing together amateur radio users, emergency managers, ESF-2 representatives, FEMA, and the RECCWGs, and to develop a process to be shared nationwide for information flow in declared disasters before the federal government gets involved. "We will use available resources such as the Communications Unit Leader (COML) curriculum and Incident Command System (ICS) course 00802 to develop contacts numbers and carrier information for priority restoration and templates for ESF-2 representatives to implement those procedures up in their area," says Victor. The Working Group will also provide education to those involved in emergency management from the incident level function and roles and above within the ESF-2 structure.

In Connecticut, Victor worked to create the ESF-2 Regional Incident Dispatcher (RID) Team in 2003, a group with 1 Coordinator, 2 Team Leaders, 2 Technical Specialists, and 16 dispatchers from 15 different communities. "All the dispatchers are versed in multi-discipline dispatching and are trained on a quarterly basis," he says. "Our communications plan calls for complete coordination and inventory of all communications assets within the region. We have set up a plan for the interoperability of all legacy systems within the region."

***If you are interested in participating in the ESF-2 Working Group, click on the Volunteer Form on NPSTC's home page.***

## Virtual USA: The Right Information, at the Right Time, for the Right People

During the Hurricane Floyd evacuation, 1.75 million people left the state via I-95 and I-75 and exited Florida into Georgia. Georgia public safety had no idea of the numbers of people and did not have adequate plans for shelter, evacuation, or traffic control. Virtual USA provides an information pipeline between different jurisdictions during such a disaster. Agencies can share live data using their own equipment. The data remains with the host agency but is available through a common platform during a disaster.

The Virtual USA website provides the data pipeline that allows partners to share critical information between geospatial viewers. The success of Virtual USA rests not only on technical capabilities, but on existing relationships among a community of emergency managers at all levels who agree to collaborate to improve situational awareness and emergency response.

Many states have built geospatial systems that provide visual images of data which can be linked to manage events. For example, the predicted paths of storms in relation to evacuation routes and gasoline supplies or the locations of schools and nursing homes to be alerted or evacuated in the case of a hazardous waste materials incident.


*The 2010 Gulf Oil Spill affected multiple states*

Emergency managers regularly face incidents that cross geographic boundaries, but are too often limited to the use of the information available only within their state or jurisdiction for response.

A storm can sweep up an entire coastline; a wildfire can send smoke and debris hundreds of miles away; a hurricane evacuation can force hundreds of thousands of people to neighboring states. In the past, emergency managers and responders would contact their colleagues in neighboring jurisdictions for information such as evacuation routes, hospital locations, or storm damage reports. If they were lucky enough to know who to call, the information received was often partial, outdated, or couldn't easily be accessed and viewed with their existing systems.

Virtual USA provides emergency managers with many different types of data from many sources. They need to be able to trust the quality of the information they are provided. They need to be able to access the information quickly, easily, and in a format that works with their system.

Virtual USA was built from the ground up by a partnership of practitioners who own these responsibilities. Together, they defined:

- How shared information should be documented and described
- The technical tools necessary to share information
- Agreements needed to set standards for sharing
- The partners that should join the sharing consortium, and
- How access to the system would be controlled

Virtual USA gives emergency managers transparency into the information that is shared, as well as control over who has access to it, where, and for how long. All shared information lists a personal point of contact, so users know who to call with questions.

Visit the VirtualUSA website for a wealth of information on how to get started in your state.

**vUSA National Information Sharing Agreement**

- vUSA National Information Sharing Agreement

**Virtual USA Pilots**

- Southeast Regional Operations Platform Pilot (SE ROPP)
  - SE ROPP Phase I Fact Sheet
  - SE ROPP Phase II Fact Sheet
  - SE ROPP Demo Information Sheet
- Pacific Northwest (PNW) Pilot

**Virtual USA Tools**

- Virtual USA: Approaches to Information Sharing
- Implementing the VIPER Information-Sharing & Visualization Platform Tool: Virginia Interoperability Picture for Emergency Response
- Virtual USA Implementation Tool

**Documents, Photos and Videos**

- Virtual USA Fact Sheet
- First Responders' Group (FRG) Fact Sheet
- Virtual USA Frequently Asked Questions (FAQ)
- White House Open Government Progress Report to the American People
- Virtual USA Privacy Considerations and Principles
- CUSEC States & DHS Demonstrate "Virtual USA" during NLE2011

## WinnF Needs Input for Technology Report to Guide Purchasing and Research Agendas

The Wireless Innovation Forum [formerly Software Defined Radio Forum] has issued a Request for Information (RFI) seeking information on current and proposed technology developments for addressing communications requirements for public safety. We are soliciting inputs from industry, academia, government researchers and users, public safety agencies, and other interested entities. The Forum's Public Safety Special Interest Group (PS SIG), which coordinates the Forum's activities that relate to public safety, will use this information for compiling a publicly available "technology assessment" report, which will be delivered to government officials in the public safety and defense community for immediate use in setting requirements for purchasing decisions and setting research agendas for making funding available.

Over the past 4 years, the PS SIG has developed a number of innovative concepts on how cognitive and other advanced radio technologies can be applied to public safety communications.[1] There is a significant amount of ongoing cognitive radio research and development in academia, as well as government and industry labs. Responses to this RFI will help the Forum assess the current state-of-the-art and maturity of cognitive and other advanced radio technologies, near-term deployment opportunities, and long-term research challenges.

The primary output of this technology assessment effort will be a report, generated by the PS SIG, directed at readers in positions of public safety community leadership, users, researchers and product developers. These responses will help set a broad research, development, and implementation agenda for the community, and will be communicated to entities such as the FCC and public safety audiences.

Organizations and individuals providing responses to this RFI will be referenced in the report for their contributions (unless they elect to remain anonymous) and thus can benefit from the enhanced exposure to their potential customers. Furthermore, these responses can help steer the direction taken by potential customers for future systems and technologies. This information will also be incorporated into the Forum's ongoing technology roadmap project.

Instructions: The survey is organized into seven sections. It is anticipated that each section can be typically be completed in 10 to 15 minutes, although longer answers are possible. PARTIAL RESPONSES ARE ACCEPTED AND COMPLETION OF MORE THAN ONE SECTION IS NOT EXPECTED. You can retake this survey as many times as you would like, providing partial responses in each section each time. Any information you can contribute is greatly valued and appreciated. Also, please include contact information that will allow members of the PS SIG to follow up in the event that clarification of a response is desired.

[1] *Wireless Innovation Forum, Use Cases for Cognitive Applications in Public Safety Communications Systems – Volume 1: Review of the 7 July Bombing of the London Underground, Report No. SDRF-07-P-0019-V1.0.0. http://groups.winnforum.org/d/do/1565.*

*Wireless Innovation Forum, Use Cases for Cognitive Applications in Public Safety Communications Systems Volume 2: Chemical Plant Explosion Scenario, Report No. WINNF-09-P-0015-V1.0.0. http://groups.winnforum.org/d/do/2325.*

## Since We Last Met

### In-Building Radio Enhancement Systems for Public Safety

The PSCR has recently published a report on in-building Bi-Directional Amplifiers (BDAs). The report "In-Building Radio Enhancement Systems for Public Safety" (IBRES) was written for public safety communication professionals tasked with assisting building owners in fulfilling in-building public safety communications requirements. The paper provides:

- Information assembled from literature search and interviews with public safety professionals and IBRES (In-Building Radio Enhancement Systems) equipment designers, manufacturers, and installers.
- A description of IBRES technology, problems endemic to it, and mitigation of these problems.
- Calculations that demonstrate IBRES effectiveness, vulnerability to strong channels, and capacity to desensitize other system repeaters.
- An experiment demonstrating BDA (bi-directional amplifier) feedback.

The paper concludes that when designed, installed, and maintained by experienced professionals, BDAs are considered reliable. Recent FCC rulings that separate low and high site systems into distinct frequency bands have greatly improved reliability. The FCC is currently working to eliminate interference from substandard BDAs.

### Agenda Released for the Fifth Canadian Public Safety Interoperability Workshop

Ottawa is the place to be from December 4 to 7 for the Fifth Canadian Public Safety Interoperability Workshop, and this year's event is shaping up to be the best ever with lots of great new speakers, workshops and new exhibitors. The agenda (just released and draft/subject to change) features:

- A Special Workshop on Social Media for Emergency Management – A "Hands On" Tutorial
- A Slave Lake Case Study
- Implementing a 700 MHz Broadband Network for Mission Critical Public Safety Data in New York City, featuring Deputy Chief Charles Dowd from NYPD
- 700 MHz for Mission Critical Public Safety Data in Canada: Why should I care?
- Arctic and Remote Interoperability – Challenges and Opportunities
- Networked/ Connected Vehicles – What it means to Public Safety Interoperability
- Communications Interoperability around the world – How Non-Governmental Organizations Manage
- Multi-Agency Situational Awareness System – Advancing on the Interoperability Continuum
- Public Private Partnership for Communications Interoperability Projects: Making it Real
- Workshops on Regional Interoperability Strategic Planning, Provincial Updates, P25 Updates, Interoperability Research

and much more!

For more information, go to http://www.cacp.ca/index/eventscontent?contentId=1048.

---

**Call to Help Shape 700 MHz Mobile Broadband Network for Emergency Responders**

Public Safety Canada's (PS) Interoperability Development Office (IDO) and the Centre for Security Science (CSS) are pleased to announce the launch of an initiative to define the Operational Requirements for 4G mobile wireless broadband services in the 700 MHz spectrum. The IDO and CSS are reaching out to the public safety community, equipment suppliers, service providers, consultants, academia, and the information and communications technology community at large for individuals interested in contributing their time and experience in this foundational effort of great importance to Canada's security and the safety of its citizens and neighbors. The requirements development process will be launched at an interactive workshop to be held on December 7, 2011 in Ottawa (immediately following the close of the Fifth Canadian Public Safety Interoperability Workshop).

Four inter-disciplinary Work Groups will be created to define the Operational Requirements for a public safety-grade wireless broadband service that will cover the following dimensions: Interoperability and Applications, Network Infrastructure, Network Management, and Security. Interested persons are kindly requested to e-mail Interoperability@ps-sp.gc.ca stating their affiliations, which Work Group they would like to participate in, and relevant experience. The closing date for receiving expressions-of-interest for Chairpersons was October 31, 2011 and for other participants is November 11, 2011. Visit the member portion of www.citig.ca for complete details.

---

**Issues to be Resolved in the 700 MHz Band**

NPSTC's Interoperability Chair, John Powell, wrote a letter to the Commission's David Furth at the Public Safety and Homeland Security Bureau in September, summarizing outstanding issues affecting 700 MHz LMR and asking for resolution. Summary points of the letter included:

(A) Clarifications and updates to Part 90 Rules and Regulations for the 700 MHz band:

- Rules for the use of analog modulation - 47 CFR 90.535(a) are not clear.
- The NAC code is not specified in the interoperability technical standards - 47 CFR 90.548(a)(1).
- Licensing "by rule" of mobiles and portables on FCC-designated interoperability channels.

(B) Summary of petitions and related issues:

- Address NPSTC 2008 Petition for 700 MHz voice clean-up.
- Designate a single voice interoperability Calling Channel in the 700 MHz band.
- Re-designate the current second Calling Channel as a National Travel Channel.
- Relax use restrictions on one of the data interoperability channels.
- Designate interoperability reserved channels for Deployable Trunked Systems.
- Revise rules on Low Power Itinerant Channels.

NPSTC's 2011 Petition for Air-Ground Interoperability Channels and the Petition on the 2017 Deadline for 6.25 kHz Narrowbanding of the 700 MHz Band are also open items.

---

**Intrinsically Safe Radio Update**

*Last fall, Factory Mutual (FM), a certification agency, announced they would be changing their IS testing process and standard in accordance with international standards. The energy constraints imposed by meeting the new FM standard will result in limiting the transmit power capabilities of LMR products. The impact of the changes will affect more than basic product design of portable radio equipment. Significant system infrastructure expansion might be necessary to maintain current geographic and in-building coverage. NPSTC became involved in resolving the issue, working with FM, the Telecommunications Industry Association (TIA), the International Society of Automation (ISA), and the Occupational Safety & Health Administration (OSHA).*

In January 2011, TIA created an engineering subcommittee (TR-8.21) to evaluate alternative solutions for operating radios in hazardous locations. The TR-8.21 considered looking at an ISA document, but rejected that because the ISA standard will be revised in 2 years, with more onerous power limits than the proposed FM revision. In June 2011, Underwriters Lab (UL) joined the TIA effort, offering its standard, UL 913.5, to TIA for consideration. This is close to the original FM standard that public safety has used to date with no problem. UL is extending this acceptable standard to 2016. They announced at the TR-8.21 meeting that they will continue to test to the UL standard if it is adopted and published by TIA.

---

**GPS Interference Update: LightSquared Must Do More Testing**

*LightSquared is a company that has spectrum in the 1.5 GHz band adjacent to the spectrum used by all Global Positioning System (GPS) receivers. LightSquared plans to build an LTE terrestrial network with approximately 40,000 sites which would provide wholesale capacity to commercial broadband providers. This could radically change and degrade the spectrum environment in which adjacent GPS signals are received, as strong signals from the LightSquared facilities could block GPS reception by public safety communications facilities and devices. NPSTC stood up the GPS Working Group to participate in the testing process.*

The GPS Technical Working Group (TWG) final report was submitted to the FCC on June 30, 2011. The report listed interference with the majority of receivers tested. The FCC opened a comment period with comments due August 15; NPSTC provided comments on July 29. The FCC requested additional test details from LightSquared (LS) on August 10, 2011. LS proposed modification of its original deployment plan on August 22. LS filed an ex parte on September 7, proposing an alternate deployment plan using only a portion of their spectrum. LS stated the alternate deployment plan would not alleviate issues with high-precision devices.

NPSTC stated that the testing was not adequate for the original or for the alternative proposals. In the meantime, the National Telecommunications and Information Administration (NTIA) filed a letter discussing their support for further testing on September 9. Neither letter defined who would be performing testing or what devices were to be tested. NPSTC believes that if testing goes forward, more public safety devices should be tested.

The FCC issued a Public Notice indicating that LightSquared must continue to test its proposed Ancillary Terrestrial Component (ATC) operations to identify and address potential interference to GPS systems those operations might cause. A technical group of over 100 participants including public safety, federal agencies and telecommunications companies tested GPS devices against LightSquared's proposed terrestrial devices and discovered the potential for harmful interference if LightSquared deployed as originally planned.

To address these concerns, LightSquared has proposed to limit its terrestrial operations to the lower 10 MHz of the band. Testing has shown that the interference potential is reduced but concerns remain for certain types of GPS receivers. Therefore, additional testing is needed and until GPS interference concerns have been satisfied, LightSquared may not deploy ATC under its waiver.

---

**Video Technology Advisory Group (VTAG)**

The VTAG was recently created to provide advice and feedback to the DHS Video Quality in Public Safety (VQiPS) Working Group. VQiPS focuses on the quality of video and the factors that affect quality, and proposes standards and guidelines for agencies to specify systems that meet their needs. To promote awareness of the video research effort and increase outreach

to end users, VQiPS sought to partner with NPSTC for advisory support. The VTAG is also able to look beyond video quality, expanding its advisory role to other issues such as interoperability and broadband.

The VTAG had its first conference call on September 21, and was asked to review a draft DHS report "Video Quality Tests for Object Recognition Applications," developed by the PSCR. ASIS, the private security industry group, has developed a handbook on video quality in security settings which the VTAG will review as well.

DHS hosts a VQiPS web tool to educate end users on the video system components. The tool provides recommendations for video technology based on use and these parameters: Usage timeframe, discrimination level, target size, motion, and lighting. VQiPS would like to strengthen the information available on the DHS web tool and is seeking information on individual components, types of radio encryption, specifications, etc. Visit the Consumer Digital Video Library at http://www.cdvl.org/. An online VQiPS video requirements web tool is now available at http://www.pscr.gov/outreach/vqips/vqips_guide/define_vid_qual_reqs.php.

---

**Filing to NIST**

The National Institute of Standards and Technology (NIST) asked for input on various possible features of a new nationwide interoperable public safety broadband network. This input will be used by NIST to help determine research and development priorities in anticipation of the President's Wireless Innovation (WIN) Fund to help drive innovation of next-generation network technologies.

In August 2010, the U.S. Department of Justice Community Oriented Policing Services (COPS) office held the National Forum on Public Safety Broadband Needs where public safety practitioners identified 15 operational requirements, each of which relate to four overarching themes: resiliency, availability and reliability, security, and affordability/commercial alignment.

NPSTC filed comments in October, thanking NIST for its assistance in helping to define beneficial research and development for the public safety broadband network. NPSTC's summary of the filing stated it is important that 1) close coordination with public safety practitioners and industry be maintained once the actual availability of research and development funding decisions are made; 2) any research and development be focused on areas where research is actually needed, not areas where existing engineering practices and operational experience already provide direction for deployments; and 3) the NIST work supplement rather than delay initial deployments of the broadband public safety network built off of the existing LTE standard. NPSTC pledges its continued involvement to assist NIST in these issues important to the public safety community.

---

**NPSTC Filings to the FCC**

NPSTC Submitted Comments on the Petition for Rulemaking (PFRM) to Allow Aircraft Voice Operations on Secondary Trunking Channels in the 700 MHz Band. July 15, 2011. NPSTC reaffirmed its support for issuance of a Notice of Proposed Rulemaking (NPRM) and urged the Commission to move forward expeditiously with an NPRM on this issue.

NPSTC Submitted Comments in Response to the Commission's Public Notice (PN) DA 11-1133, Regarding LightSquared Technical Working Group Report. July 29, 2011. NPSTC addressed issues surrounding potential interference to public safety use of GPS and provided recommendations for additional testing under the modified deployment approach LightSquared proposed in its recommendations submitted June 30, 2011.

NPSTC Submitted Comments in Response to the FCC's PN on a Sprint Nextel 800 MHz Petition. August 1, 2011. NPSTC recommended the Commission allow commercial wideband or broadband operations to be deployed in the ESMR (Enhanced Specialized Mobile Radio) bands only in regions in which rebanding of the 800 MHz NPSPAC (National Public Safety Planning Advisory Committee) channels has been completed and where such wideband use would not interfere with public safety NPSPAC operations not yet rebanded in adjacent regions.

NPSTC Submitted Reply Comments in Response to the FCC's Rules to Improve Wireless Coverage Using Signal Boosters. August 24, 2011. NPSTC recommended the Commission grandfather existing Class B signal boosters in the Part 90 services

for 10 years and consider implementing a process under which public safety entities could deploy new Class B boosters only on an exception basis through frequency coordination and licensing.

NPSTC Filed an Ex Parte Letter with the FCC on the 700 MHz Band Cleanup. September 11, 2011. NPSTC detailed the unresolved issues in the 700 MHz band, asking for action.