

**Greg Brown, Co-CEO, Motorola**  
**National Governor's Association Annual Meeting**  
**Plenary Session on Emergency Preparedness**  
**Sunday, July 19, 2009**

Thank you governors for keeping focus, and thank you for the opportunity to speak to you today. I would like to particularly thank Governor Barbour who ensured that this topic be on the meeting's agenda today. And as Governor Rendell says in the report *Infrastructure Vision for the 21<sup>st</sup> Century*, quote "infrastructure is the backbone of our society." As the report states, our country's infrastructure has not kept pace with our country's growth and shifting demands. The nation's governors have been presented with a unique opportunity through the American Recovery and Re-investment Act to address our nation's infrastructure challenges, not only in terms of modernization and repair, but also in the areas of emergency preparedness. Let me give you a few quick examples:

First, Congress gave governors, at your urging, the discretion to at least use a portion of the State Fiscal Stabilization Fund for public safety or other government services. This amounts to about \$8.8 billion national wide. Some governors are already planning to use a portion of their so called government services fund allocations for public safety technology. I would urge you to balance your short term needs related to filling budget gaps with using at least a portion of this one-time funding for long term investment in completing or making measurable progress towards achieving your state's interoperability objectives.

Second, an unprecedented level of funding, about \$7 billion, has been made available for broadband infrastructure in un-served and under-served areas, and Congress has specifically included public safety access to broadband services as one of its objectives. The grant guidance for the first round of funding programs being administered by NTIA and the Rural Utility Service was just recently released but I think there is an opportunity there.

Third, \$2 billion was made available for the Byrne Justice Assistance Program. This is the high watermark for this program, which can be used for a broad range of law enforcement purposes, including technologies. States have discretion over how 60% of this funding is used.

Fourth, there is another \$300 million available through FEMA for port security and transit security which can include technology investment, such as video surveillance to protect that critical infrastructure.

In a similar vein, there are numerous programs in the Recovery Act under which technology investments can be made to protect infrastructure and enhance safety. Highway money can be used for intelligent transportation solutions that enhance safety and facilitate preparedness. Education money can be used for campus security. Health IT money will make hospitals better prepared to handle mass

**Greg Brown, Co-CEO, Motorola**  
**National Governor's Association Annual Meeting**  
**Plenary Session on Emergency Preparedness**  
**Sunday, July 19, 2009**

emergencies. So with the Recovery Act, you have a unique opportunity to leverage some of these funds for the critical infrastructure needed for emergency preparedness. Now that said, it doesn't change the fact that you all have the mandate for annual balanced budgets, and undoubtedly the heavy lifting in the funding for state infrastructure modernization around communications and emergency preparedness comes from the state.

Now, in terms of emergency preparedness, when we look at the topic, it covers disaster response, planning, securing our nation's borders and ports, and even emerging threats such a cyber security, which are borderless. Emergency preparedness cannot function without wired and wireless communications. It's like oxygen; without it, nothing happens. Voice and data communications capabilities must survive disasters and emergencies. As a fellow CEO, I can relate to the enormous challenges you face as CEOs of your respective states in finding the resources in this economic climate to balance your numerous priorities within the area of emergency preparedness and keeping your state safe for the public. Technology is the mechanism to deliver the various systems of government you manage as CEOs of your states, including both the prevention and response sides of emergency preparedness. I believe states can balances the priorities and address emergency preparedness in a cost effective manner by taking an enterprise wide approach to your technology infrastructure. And by that I mean, as we have seen over the last several years, more and more states – and to date, 34 states- have taken a state-wide approach for efficiencies, effectiveness, state, local, county, etc. for the interoperability and survivability of emergency communications. An enterprise wide approach enables you to take a holistic view of your technology needs and look across the regions in both public safety and public service sectors, and to assess your requirements to meet the goals of prevention and response. With any enterprise in the public safety realm, you need to invest in multiple types of technology in order to satisfy the needs of your users. Within the public safety enterprise your users have three key requirements that are the same across all of your agencies:

One is seamless connectivity. Your entire enterprise requires broadband communications networks both wireless and wireline, both public and private. Mission critical voice and data communications is critical, both for the prevention and in times of response, to ensure the safety of your states. Broadband communications networks should be considered part of our nation's core infrastructure just as roads, transit systems, education systems, and hospitals are. We are in support of the Administration's call for a national broadband strategy.

**Greg Brown, Co-CEO, Motorola**  
**National Governor's Association Annual Meeting**  
**Plenary Session on Emergency Preparedness**  
**Sunday, July 19, 2009**

Second is real time information. Secretary Napolitano talked about information and intelligence sharing and her movement towards fusion centers. Your public safety and agency personnel need information in real time to assess situations. Getting information to them in real time requires not only seamless connectivity; it requires mobile applications, wireless video, and command centers to make it possible. As an example, Los Angeles Police Department saw a 40% reduction in crime when they began using mobile video surveillance over a wireless broadband network in Jordan Downs, one of the city's most dangerous areas.

Third requirement in the hands of users: in addition to getting them real time information to assess situations, the information has to get into the right hands. Getting real time information into the hands of users is possible through mission critical two-way radios, in-vehicle computers, and mobile computers. The type of device should be tailored to the type of user. As with any enterprise, insuring your technology investments that are interoperable with other agencies using different technologies and compatible with existing systems should be both a budgeting and planning priority. Interoperability across networks enables interagency communications, ensures real time information, and gets this information in the hands of your users when they need it. Backward and forward compatibility minimizes risk to prior and future investments. And in addition, better spectrum utilization, data sharing, and integrated security positively affects total cost of ownership and improves the effectiveness of your state's workforce. Our own experience, as was referenced with public safety, is that mission critical technologies are vital to emergency preparedness. We have seen this in real time – Katrina was clearly our largest single disaster recovery response, as I am sure it was for all of the other companies affected. Although we provided personnel and equipment and more, to Governor Barbour's opening remarks and referencing the Civil War, it was like overnight going from an interconnected communicating infrastructure to overnight waking up to what felt like a Third World country, and what has to be done on the very fundamental blocking and tackling things that are necessary. It is a different thought; it is a different mentality. I remember asking questions about what was deployed, where it was deployed, and where it was invested, and were there redundant systems? What about battery backup? But if the battery backup that has been invested in is deployed a mile over in a basement that is also flooding, the investment is useless. So I think that there are a lot of lessons learned around deployment, planning, best practices that are indifferent and absent technology that we all could grow and use in an advantaged way going forward.

**Greg Brown, Co-CEO, Motorola**  
**National Governor's Association Annual Meeting**  
**Plenary Session on Emergency Preparedness**  
**Sunday, July 19, 2009**

We saw in practice the true benefits of interagency communications when state troopers from Michigan were able to use their P25 two-way radios on the state of Louisiana network, which allowed a more beneficial mutual aid response. At the Minnesota bridge collapse, we saw a single 800 Megahertz radio communication system used by first responders during the bridge collapse, and 74 different agencies during the rescue and recovery effort, providing seamless interoperable communications for first responders from several different jurisdictions throughout the area. With the California wildfires, same thing – there were radios, and batteries and other communications supplied but a whole host of very well thought through processes that allowed a very efficient and strong response to those hazards.

In terms of lessons learned, I think the most obvious, given the immense variety of emergency types, it is most important to retain an all-hazards approach to emergency preparedness, which is exactly what FEMA has done, and I am sure Administrator Fugate will address, we heard Governor Barbour and Secretary Napolitano reference, the potential for regulations and policies to be actively reviewed, which we know are being done and potentially having hazard mitigation funds available could go a long way.

Second, there is a direct correlation between restoration and preparedness. Exercises, drills, scenario planning, keeping contact information updated, prepositioning equipment, knowing what you can count on vendors to do before and after an event will greatly facilitate the recovery process. In other words, inspect what you expect and there is no short cut around training.

Third, it is very important to have network monitoring of mission critical systems and applications which can provide early diagnoses of problems, track storms and outages, and provide proactive damage assessment. This also helps reduce costs, enabling problems to be corrected remotely without the need for field personnel, and when personnel are deployed, it makes them more efficient by providing the backup technical support they need.

Fourth, existing assets should be hardened. Plan for the worst. For example, prior to Hurricane Katrina, towers, shelters, etc. were built for a Category 3 specification but post-Katrina, we are building to a Category 5 specification.

Fifth, primary networks should be augmented with alternative technologies such as mesh networking and/or satellite, and/or cellular. Similarly, alternate energy should be available, such as portable fuel cells.

**Greg Brown, Co-CEO, Motorola**  
**National Governor's Association Annual Meeting**  
**Plenary Session on Emergency Preparedness**  
**Sunday, July 19, 2009**

Finally and perhaps most importantly, this is a subject I have already touched on but the subject of true interoperability. It is non-negotiable. Interoperability provides the means to positively and effectively manage situations both in crisis mode and response mode but also in the prevention mode. The P25 Standard, which was jointly developed by the public safety user representatives as well as the Telecommunications Industry Association, includes participation from equipment manufacturers and is an open industry standard. Therefore it does not represent a specific technology, but it does represent reliable requirements for voice, data, and video communications.

So the technology to solve the challenge of interoperability and interagency communications exists today, but in many instances, the main impediment to implementing it is funding. States should be given maximum flexibility to use their disaster mitigation dollars for the prevention of disasters and for use in upgrading current communications systems to the open standard nationally and federally and state and local defined P25 based systems. As governors, I urge you to make the case to the federal government for support in upgrading our nation's public safety communications infrastructure just as they are doing for roads, schools, and hospitals. Somewhat I think that interoperability has been solved because of the significant investments that have been made since 9/11, but I don't have to tell you that I think there remains much to be done. While we have talked a lot about Katrina today, there is one emergency situation where the use of P25 communications devices was extremely beneficial because interagency communications was possible and real. And earlier I gave the example of Michigan state troopers bringing their P25 devices to Louisiana and being able to communicate with other safety agencies. In a time when communications was barely possible interagency, this was a huge benefit to all. A parallel example of this is email. Once standards enabled various proprietary email systems to be fully interoperable, email usage flourished and became the indispensable tool that it is today. So again, I urge you to continue to make the case to the Federal Government for funding and for flexibility in using disaster mitigation dollars for technology both for prevention and response.

In terms of cybersecurity which was mentioned, we have to do more in terms of public and private partnership. I have the privilege of being one of thirty CEOs from the high-tech industry to serve on the President's Administration NSTAC Committee with recommendations on assuring vital communications links through any event or crisis. But I will tell you that cybersecurity, while talked about significantly and with President Obama highlighting it in a press conference about four weeks ago, it is a national issue. And yes, there are steps that can be taken at

**Greg Brown, Co-CEO, Motorola**  
**National Governor's Association Annual Meeting**  
**Plenary Session on Emergency Preparedness**  
**Sunday, July 19, 2009**

the federal level, but it's a state and local coordinated effort as well. And I think with some of the national association state CIOs that you all have in place, some good coordinating work will be done on that.

Lastly, I just leave you with one final thought. People ask me, with different budget situations, priorities within states, pretty much a ubiquitous shortage of funds, Greg – what are the common attributes that are there when states successfully implement a state-of-the-art interoperability communications system? And I think the number one requirement is you. Because when a governor takes a leadership role, and he or she makes it a priority, and then determines and declares that as a top priority to your respective administration and constituents, things happen significantly. So putting the state on the path to an enterprise-wide approach to technology investment, establishing the proper governance framework, bringing different stakeholders together, I was thrilled to see the NGA's proposed new policy position on public safety communications and the explicit recognition and the need for public and private sector coordination. I really appreciate you highlighting this on the agenda and your continued courage and leadership making this a priority.

Thank you.