

AS PREPARED FOR DELIVERY

James Arden Barnett, Jr., Rear Admiral (Ret.)
Chief, Public Safety & Homeland Security Bureau
Federal Communications Commission

Homeland Infrastructure Foundation-Level Data
Working Group Bi-Monthly Meeting

November 1, 2010
8:30 AM-9:00 AM
FCC Headquarters
CMR

Let me reiterate what Steve said, and welcome you to the Federal Communications Commission. I'm honored to have been asked to speak with you today, and it's truly a pleasure to be in front of such an esteemed group.

In light of the fact it's football season, I have to throw a football quote in here... Vince Lombardi once said, "People who work together will win, whether it be against complex football defenses, or the problems of modern society." How right he was. The Homeland Infrastructure Foundation-Level Data Working Group epitomizes the value of teamwork conveyed in Coach Lombardi's words. Your group strives to improve collaboration among multiple levels of government and the private sector in the collection, processing and protection of critical infrastructure geospatial information which can aid all of us if and when a man-made or natural disaster occurs. The FCC is proud to be a part of this effort.

We understand the importance of collaborating in order to create synergistic working relationships and databases before tragic events occur. It's critical that when disaster strikes, we have as much information at our fingertips as possible and that we know what the data means, how to

interpret it and how to use it. The only way to efficiently gather and effectively utilize such a vast amount of information is through planning and partnerships.

The Public Safety and Homeland Security Bureau strongly believes in building effective collaborations and believes that working together is a large part of making our communities safer places to live and work. I realize that some of you may not be familiar with the Bureau, so I'd like to take a few minutes to tell you a little bit about us.

I was named Bureau Chief about a year and a half ago by Chairman Genachowski and it has proven to be an exciting assignment. As Bureau Chief, I get to lead the team responsible for carrying out the Commission's public safety mission, focusing on the development of rapid, reliable, and ubiquitous communications technologies to promote public safety and homeland security. Created in 2006 following Hurricane Katrina, the Bureau focuses on areas such as broadband technologies, 9-1-1 services, interoperability, protecting communications infrastructure, cyber security, ensuring the availability of communications as part of emergency preparedness and disaster response, and

outreach on communications issues to the public safety community. To that end, we work closely with the first responder community, including police, fire and emergency medical agencies; emergency operations centers; public safety answering points; hospitals; state, tribal, and local governments; and other Federal agencies. We interact on a daily basis with public safety personnel that operate state, local, and tribal police, fire, and emergency medical radio systems, and we also play a role in emergency preparedness and response. Partnering with FEMA, we deploy FCC staff in advance of or following disasters to assist with communications assessments and recovery.

As you are well aware, in disasters and other emergency management situations, situational awareness is paramount to the incident management community whether they be local first responders on the scene initially or subsequent state or federal responders. A common operating picture that can be shared among all responders is the key to an interoperable community for responders, and it is critical for a common operating environment to be based on a foundation of verified location information. This is especially true for those elements of the picture that form our

critical infrastructure and, without a doubt, the communications industry is a significant component of those critical resources.

We only need to recall such major incidents as Hurricane Katrina and the attacks on the World Trade Center and the Pentagon to recognize the importance of a common operating picture that recognizes the location of critical communications nodes and facilities. Within the communications domain, these critical elements include the locations of switches, SS7 control switches, critical point-to-point radio transmitters, satellite earth stations, undersea cable landings, and other essential communications facilities. Correspondingly, it is essential that our common operating picture reflects the condition of these communications facilities and is able to identify which facilities are available or which assets have been impacted by the incident. The ability of our communications carriers to respond to the attacks in New York on 9/11 substantiates the need for this critical infrastructure information in that it allowed for the rapid reconstitution of services in the financial district – a feat that was dependent on assessing the availability of critical resources to support the reconstitution.

However, accurate asset location information is important for more than just being able to respond and recover. It is also necessary to perform risk assessment(s) and risk management even before any potential incident. The ability to accurately locate key resources and critical installations is essential to any risk management process and is just plain common sense in any critical infrastructure protection plan. It lets us prepare in advance so that we can minimize any potential harm that may occur. This is extremely important when one considers the large task that governments at all levels face in coordinating their essential functions and interdependencies.

On another emergency preparedness and response note, PSHSB is responsible for developing and operating a system we call "Roll-Call." Roll-Call is a national asset that can best be described as a spectrum analyzer on a truck. When Roll-Call moves into a disaster area, it can determine if there is anyone broadcasting in various frequencies. As a result, it can determine whether broadcast stations, public safety land mobile radio (LMR) facilities, and US government unclassified LMR are operating. The locations and frequencies of all the equipment that are within range of Roll-

Call are in location databases that PSHSB gets from Don Campbell in the FCC's Office of Engineering and Technology, and he will be talking more about this in more detail tomorrow afternoon along with Jim Pierson of PSHSB. Roll Call was used during Hurricanes Ike and Gustav and was recently utilized in Haiti to check the status of communications networks after the tragic earthquake there. We are proud of Roll Call and the benefits that system provides to our Federal, state and local partners when needed.

As I mentioned earlier, in order for us to adequately respond to and recover from disasters, we have to know what assets we have, and whether or not they are working properly. Accordingly, in order to ensure as complete a picture as possible, PSHSB also collects data on network outages reported by carriers in accordance with Part 4 of our rules. We have been collecting this data since the beginning of 2005. After analysis by our technical experts the data is stored in a database called the Network Outage Reporting System (NORS). This data includes not only the physical location of the outage, but additional information regarding what went wrong and why, and what steps have been taken

to prevent similar outages from occurring in the future. While NORS does not include all outages impacting the communications infrastructure, it does include the vast majority. We use the location of the reported outage to identify outages that affect more than one company. We have seen single cable cuts that have affected customers and Public Safety Answering Points (PSAPs) hundreds of miles away from the breach. Knowing the location of communications assets is essential to understanding the full effects of an outage and aids us in our ability to determine whether architecture improvements could mitigate the effects of failures.

On another note, as we move toward a world that relies more and more on the internet and broadband applications, we must remember that access to IP services affects the resiliency of the communications infrastructure. Therefore, knowing the location of critical IP assets and their strengths and weaknesses is essential to preparing for and/or preventing failures of those types of services.

Cybersecurity is one of the most important issues on which we are currently focused. We are working with other

federal departments and agencies to do all we can to improve the country's efforts related to this critical issue. It can appear to be a daunting task, but working together, we can ensure that our Nation has a safe and secure communications network.

And, by the way, let me put a plug in here for an event we have coming up on November 5 that will focus on cybersecurity. The National Broadband Plan included a recommendation that the FCC issue a Cybersecurity Roadmap to identify the five most critical cybersecurity threats to the communications infrastructure and its end users and recommend a plan for the FCC to address these threats. The workshop on November 5 is intended to provide the FCC with input on key issues in the development of the FCC's Cybersecurity Roadmap. We would welcome your input on this extremely important topic, so I invite you to participate in this event either in person here at the FCC or via the web.

I hope my remarks today have reinforced the idea that communications and other sectors are intimately connected and that we are all in this endeavor together. I give the

HIFLD working group kudos for seeing the importance of these concepts years ago and for taking the steps to create synergistic relationships that work toward furthering our country's preparedness.

Let me again say welcome to the FCC. I hope your meeting goes well and that we continue to build upon the work we've started. Thank you for your commitment to the country's preparedness and for the sacrifices you make to ensure we are ready for the next event, whenever that may be.