AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 109–1095

# AN INTEGRATED NATIONAL ALL-HAZARDS ALERT SYSTEM

## HEARING

BEFORE THE

SUBCOMMITTEE ON DISASTER PREVENTION AND PREDICTION

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JULY 27, 2005

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

62–408 PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office,
http://bookstore.gpo.gov. For more information, contact the GPO Customer Contact Center,
U.S. Government Printing Office. Phone 202–512–1800, or 866–512–1800 (toll-free). E-mail, gpo@custhelp.com.

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

TED STEVENS, Alaska, *Chairman*

JOHN McCAIN, Arizona
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
GORDON H. SMITH, Oregon
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire
JIM DeMINT, South Carolina
DAVID VITTER, Louisiana

DANIEL K. INOUYE, Hawaii, *Co-Chairman*
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
E. BENJAMIN NELSON, Nebraska
MARK PRYOR, Arkansas

LISA J. SUTHERLAND, *Republican Staff Director*
CHRISTINE DRAGER KURTH, *Republican Deputy Staff Director*
DAVID RUSSELL, *Republican Chief Counsel*
MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
SAMUEL E. WHITEHORN, *Democratic Deputy Staff Director and General Counsel*
LILA HARPER HELMS, *Democratic Policy Director*

---

SUBCOMMITTEE ON DISASTER PREVENTION AND PREDICTION

JIM DeMINT, South Carolina, *Chairman*
TED STEVENS, Alaska
GORDON H. SMITH, Oregon
DAVID VITTER, Louisiana

E. BENJAMIN NELSON, Nebraska, *Ranking*
MARIA CANTWELL, Washington
BILL NELSON, Florida

# CONTENTS


| | Page |
|---|---|
| Hearing held on July 27, 2005 | 1 |
| Statement of Senator DeMint | 1 |
| Statement of Senator E. Benjamin Nelson | 2 |
| Statement of Senator Stevens | 17 |

WITNESSES

| | |
|---|---|
| Hoover, Reynold N., Director, Office of National Security Coordination, Federal Emergency Management Agency (FEMA), Department of Homeland Security | 4 |
| Prepared statement | 6 |
| Lawson, John M., President/CEO, Association of Public Television Stations | 26 |
| Prepared statement | 28 |
| Guttman-McCabe, Christopher, Assistant Vice President, Homeland Security and Regulatory Policy, CTIA—The Wireless Association™ | 32 |
| Prepared statement | 33 |
| Moran, Kenneth, Acting Director, Office of Homeland Security Enforcement Bureau, Federal Communications Commission (FCC) | 8 |
| Prepared statement | 9 |
| Paese, Mark, Director, Maintenance, Logistics and Acquisition Division, National Weather Service, National Oceanic and Atmospheric Administration (NOAA) | 12 |
| Prepared statement | 14 |
| Taylor, Richard, Executive Director, North Carolina Wireless 911 Board; Chairman, the COMCARE Alliance and E–911 Institute; Partner, the National Emergency Alerting and Response Systems Initiative (NEARS) | 37 |
| Prepared statement | 38 |

APPENDIX

| | |
|---|---|
| Inouye, Hon. Daniel K., U.S. Senator from Hawaii, prepared statement | 55 |

# AN INTEGRATED NATIONAL ALL–HAZARDS ALERT SYSTEM

**WEDNESDAY, JULY 27, 2005**

U.S. SENATE,
SUBCOMMITTEE ON DISASTER PREVENTION AND PREDICTION,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
*Washington, DC.*

The Subcommittee met, pursuant to notice, at 10:05 a.m. in room SR–253, Russell Senate Office Building, Hon. Jim DeMint, Chairman of the Subcommittee, presiding.

## OPENING STATEMENT OF HON. JIM DEMINT, U.S. SENATOR FROM SOUTH CAROLINA

Senator DEMINT. Good morning. I want to thank everyone for coming. We've got other Members, including our Ranking Member, on the way, but, in deference to those who are here, let's get started with this hearing.

Somewhere in America today, a community will likely be impacted by a disaster, be it an accidental manmade disaster or a natural disaster of some sort. And as the tragic events in Britain and Egypt have shown us, the threat of a terrorist disaster still looms large. Regardless of the nature or scale of these disasters, the Nation's emergency responders need the capability to promptly and effectively communicate with the citizens in their communities.

For a number of years, America has employed a variety of alerting methods; most notably, the Emergency Broadcast System and the NOAA Weather Radio. These systems have saved numerous lives. But in this increasingly wired and wireless world, we need to be aware that if we're going to communicate more effectively with citizens, we need to look hard at modernizing and improving the system. This means moving beyond the hodgepodge of alerting technologies that are spread throughout Federal agencies. It will mean increasing coordination with state and local governments, beyond what we do today. It will require the Federal Government to move out of the analog era and embrace the digital revolution.

This will not be the work of the Federal Government, alone. If this system is truly to be an effective tool to alert the public, it must continue to embrace the public-private partnership that has served the system well in the past.

For the past five decades, the public alert system has effectively separated the generation of alerts from the actual dissemination of alerts. It has always been, and should continue to be, the responsibility of the government to assess the threat and generate an alert.

This is clearly a core responsibility of the local, State, and Federal governments, and there should be no liability for carriers who transmit these alerts to citizens.

The actual distribution of the alerts should remain with the private sector. The broadcasting community has been extremely cooperative with governments in delivering alerts. Their cooperation has been a true public service. I am optimistic this cooperation will continue as the next-generation system develops.

I'm looking forward to the testimony of our witnesses this morning. Appearing before the Committee this morning are representatives of the Federal Emergency Management Agency, the Federal Communications Commission, and the NOAA Weather Services to discuss how the various agencies of the Federal Government are working together to improve the Federal Government's alerting capabilities and to improve the current analog system.

I'm also looking forward to the comments of our private-sector witnesses. As I mentioned earlier, the private sector is going to play an essential role in making sure the system works. I'm interested in getting an assessment from the cellular industry on how we can work with them to ensure their subscribers are alerted to potential threats. I'm also looking forward to reviewing the capabilities of the DTV towers to transmit data and information to our communities in a time of crisis. Finally, it's the first-responders who are going to be charged with responding to a crisis, and I look forward to hearing from them on what type of tools they need to communicate with the public.

This hearing is essential. The Committee is moving forward with developing a National All-Hazards Alert System. Legislation is being developed now. The system is too important to the Nation not to get it right. The input of today's witnesses will provide us with the guidelines for a system that will serve the Nation well. When we get the system right, it will help protect our citizens from the threat posed by natural and manmade disasters.

With that, I yield to my Ranking Member for any opening comments he may have, and then I'd like to introduce our first panel of witnesses.

**STATEMENT OF HON. E. BENJAMIN NELSON, U.S. SENATOR FROM NEBRASKA**

Senator BEN NELSON. Thank you, Mr. Chairman.

First, I want to thank you for bringing together the witnesses and calling this hearing today. I want to thank all the witnesses, as well. It's an important issue, as the Chairman has indicated, and I appreciate your taking time to be here today to enlighten us.

When our Nation's system of alerts was first established, it was in response to the threat of a possible attack from another nation. Now, today Americans rely on a patchwork of largely voluntary systems to inform them of a range of hazards, from thunderstorms and tornadoes, to AMBER Alerts, to acts of terrorism.

While several efforts are currently underway by various government agencies to make this system of public warnings more useful and timely, we're still relying on this patchwork of technologies and methods of dissemination. To be effective, though, a warning system must be able to detect a hazard, disseminate a warning, and

suggest a response in a timely fashion. For predictable long-lead-time hazards, like hurricanes, the current warning system seems to be relatively effective. But for hazards with little or no lead time, like a tsunami or tornadoes or acts of terrorism, we must ensure that the delivery of emergency alerts is both effective and timely.

In addition, the systems used to transmit these warnings must be reliable and include redundant facilities to ensure that notification is not disrupted or hampered by inadequate systems or damage to infrastructure.

Chairman DeMint, I thank you for this hearing, and I look forward to hearing more about what our Federal agencies are doing to better coordinate their efforts to make these warning systems more robust and cohesive. I think it's important that we be aware of our shortcomings, at the same time, though, in this area.

This hearing will, hopefully, help us to learn more about what Congress can do to help all of you who are working to make sure that we have these systems and help deliver the best warning system possible. I hope this hearing will focus our attention on what technologies we can, and should, be taking advantage of to ensure the safety of our citizens. But, at the same time, I hope we will not become so enamored by the most cutting-edge advanced technologies that we forget the common-sense things that we can do to make sure that warnings reach all people, whether we're in a large metropolitan area or someone working in a cornfield.

I look forward to the testimony, and I'm anxious to hear the witnesses.

Thank you very much, Mr. Chairman.

Senator DEMINT. Thank you, Senator Nelson.

Appearing before the Subcommittee this morning is Mr. Reynold Hoover. Mr. Hoover is the Director of the Office of National Security Coordination at FEMA. Mr. Hoover's office is the program manager for the Integrated Public Alert and Warning System Project, and he will be discussing the result of phase one of the project, and plans for phase two.

Joining him is Mr. Mark Paese, Director of Maintenance, Logistics, and Acquisition Services at the National Weather Service. Mr. Paese will be discussing the NOAA Weather Radio System and NOAA's work to improve and modernize the system.

Finally, on this panel is Mr. Kenneth Moran, and he's the Acting Director of the Office of Homeland Security at the Federal Communication Commission. Mr. Moran will discuss the Commission's recent notice of proposed rulemaking on improvements of the Emergency Alert System and the comments the Commission has received.

With that, I'll start with Mr. Hoover. Mr. Hoover, if you will please provide a short summary. These lights will be your guide. I think you have 5 minutes. And the red lights indicates you might be going over. And we will appreciate your comments. Thank you.

**STATEMENT OF REYNOLD N. HOOVER, DIRECTOR, OFFICE OF NATIONAL SECURITY COORDINATION, FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA), DEPARTMENT OF HOMELAND SECURITY**

Mr. HOOVER. Thank you, Mr. Chairman.

Good morning, Chairman DeMint and members of the Committee. My name is Reynold Hoover. I'm the Director of the Office of National Security Coordination in the Federal Emergency Management Agency, FEMA, which, as you know, is a part of the Department of Homeland Security.

Thank you for the opportunity to appear before you today to discuss the role and activities in the Department of Homeland Security and FEMA to support the important mission of public alert and warning using an Integrated Public Alert and Warning System, or IPAWS, approach. FEMA, through my office, serves as the Lead Agent for the Federal Government's continuity of operations and continuity of government programs, as the Executive Agent for the national-level Emergency Alert System, or EAS, and the Department's Program Manager for the Integrated Public Alert and Warning System Initiative.

This morning, I'd like to take a few moments to tell you how the Department and our partners are improving and building an enhanced capability to provide nationwide all-hazards alert and warning using digital and other cutting-edge technologies in an integrated and coordinated manner.

The current EAS system is designed to provide the President the capability to transmit to the nation, within 10 minutes, from any location at any time. State and local emergency managers can, and do, activate the EAS for state and local public alert and warning messages, such as AMBER Alerts, hazardous-material incidents, and severe weather warnings.

With that as a point of reference, let me briefly describe to you and the Committee our efforts toward building a next-generation, all-hazards alert and warning system.

This fiscal year, we began a digital alert and warning system pilot in the national capital region with the Association of Public Television Stations. Significantly, through the voluntary cooperation and full participation of public and commercial broadcasters, satellite radio, the cellular telephone industry, technology developers, pager service providers, cable operators and others, we have successfully demonstrated an ability to transmit a variety of alert and warning messages via digital television and satellite to a full range of retransmission medium using a common alerting protocol. We are especially pleased that NOAA and the FCC have been full partners with us in this digital alert and warning pilot.

This pilot has enabled us to establish a foundation for a unified national all-hazards system and, building upon the success in the national capital region, we're moving the digital EAS pilot into a second phase of testing and development to demonstrate a national capability, identify technological challenges, and develop a nationwide implementation plan.

Because the next-generation national warning system must incorporate an ability to deliver a message to a precise group, we have partnered with NOAA to pilot a Geo-Targeted Alerting Sys-

tem, called GTAS, under the IPAWS umbrella to demonstrate the ability to provide geographically-targeted warnings.

Mr. Chairman, our IPAWS solution recognizes the ubiquity of the Internet and the powerful tool it can be in our national toolbox of alert and warning systems. In that regard, we are finalizing a cooperative agreement with the National Association of State Chief Information Officers to pilot an AMBER-Alert-like portal for all-hazards alert and warning. This effort will build upon the success and lessons learned that the Department of Justice has demonstrated in providing an effective web-portal solution for its AMBER Alert Program.

In order to assure connectivity for Presidential emergency messages, we are upgrading the Primary Entry Point, or PEP, system as part of the IPAWS to a satellite distribution system, and we'll be expanding the number of PEP broadcast stations so that each state and territory will have a direct satellite-receive capability. By leveraging public-private partnerships, these critical upgrades will ensure the survivability of radio broadcast systems in the event of a catastrophic attack on the homeland.

And we recognize, Mr. Chairman, that there is no single solution set that will meet everyone's alert and warning requirements. That's why we are seeking the most appropriate interoperable solutions to develop the Integrated Public Alert and Warning System approach.

We believe that IPAWS, using digital technology, in combination with upgraded Primary Entry Point EAS capabilities, will provide Federal, state, and local emergency managers and leaders with the tools they need to protect America from both manmade and natural disasters. But, more importantly, the IPAWS solution is intended to complement, not compete or interfere with, existing alert and warning systems. Moreover, the IPAWS is based upon the premise of providing alert and warning messaging in a coordinated manner over as many platforms as possible to ensure the widest public dissemination and receive capabilities.

Of equal importance, we are reaching out to stakeholders and alert and warning system users through a series of IPAWS seminars. Significantly, our most recent seminar included representatives from the disabled community who told us about the challenges they face with regard to alert and warning. As we continue that dialogue, we will incorporate their concerns with IPAWS solutions.

Mr. Chairman, these are just some of the examples of how FEMA and the Department of Homeland Security have taken seriously its responsibility to ensure quick and accurate dissemination of alert and warning information to our homeland security partners and to the American public.

Thank you, again, for the invitation to speak and for your support of the Department's mission and for your interest in an effective next-generation all-hazards alert and warning system. And I'll be pleased to answer any questions you may have.

[The prepared statement of Mr. Hoover follows:]

PREPARED STATEMENT OF REYNOLD N. HOOVER, DIRECTOR, OFFICE OF NATIONAL SECURITY COORDINATION, FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA), DEPARTMENT OF HOMELAND SECURITY

Good morning, Chairman DeMint and members of the Committee. I am Reynold N. Hoover, the Director of the Office of National Security Coordination (ONSC) within the Federal Emergency Management Agency (FEMA). Thank you for the opportunity to appear before you today to discuss the role and activities of the Department of Homeland Security and FEMA to support the important mission of public alert and warning using an Integrated Public Alert and Warning System (IPAWS) approach.

FEMA, through my office, serves as the lead agent for the Federal Executive Branch's Continuity of Operations (COOP) and Continuity of Government (COG) programs and as the Executive Agent for the national-level Emergency Alert System (EAS). Our office also functions as the Department's Program Manager for the IPAWS initiative of which EAS is a component. As such, we are working in close cooperation with the Information Analysis and Infrastructure Protection (IAIP) Directorate to facilitate coordinated efforts within the Department. I also serve as one of the managing Co-Chairs of the White House Task Force on Effective Warning that was chartered by the Office of Science Technology and Policy and Homeland Security Council. This recently established Task Force has representation from key public alert and warning stakeholders in the Federal Executive Branch and is Co-Chaired by the National Oceanic and Atmospheric Administration (NOAA). On all of these public alert and warning initiatives, we share close relationships with the Federal Communications Commission (FCC) which generally regulates EAS technical standards, procedures and protocols, and with NOAA which is a primary EAS user.

We appreciate the Alert and Warning funds Congress has provided to the Department to improve our alert and warning capabilities. Your funding will help us provide Americans with critical and timely information alerts and warnings that will save lives and property. This morning I would like to take a few moments to tell you about the EAS and IPAWS which is the foundation upon which the Department is improving, and building, an enhanced capability to provide nationwide alert and warning using cutting edge technologies, in an integrated and coordinated manner.

The EAS in its current form was established in 1994 and is essentially a cascade, trickle down, distribution system from the FEMA Operations Centers to 34 designated Primary Entry Point (PEP) radio broadcast stations. At the request of the President, we distribute a Presidential level message to the PEP stations, which in turn re-broadcast the signal to monitoring stations down stream which then broadcast the message over TV and radios. The system is designed to provide the President the capability to transmit within 10 minutes from any location at any time. This Presidential message is mandatory, must take priority over any other message and must preempt other messages in progress. All other broadcasts of emergency messages are voluntary. Nevertheless, state and local emergency managers can, and do, activate the EAS for state and local public alert and warning messages such as AMBER alerts, hazardous material incidents and weather warnings. NOAA, and the National Weather Service, serve as the originator of emergency weather information, and play a significant role in the implementation of EAS at the state and local level. While FEMA tests on a weekly basis the connectivity to the 34 PEP stations, the national level EAS has never been fully activated.

As you are well aware, the tragic events of September 11 caused a paradigm shift in how we think about homeland security and, in particular, alert and warning. As efficient and useful as the EAS has been, we in FEMA and the Department of Homeland Security realize that the alert and warning system that so many millions of people depend upon is not everything to everyone all of the time. With the alert and warning funding provided this year, FEMA, IAIP and our partners in the Federal Government are making great progress in our ability to reach more of the people, more of the time. We believe in a very short period of time, leveraging public-private partnerships and using existing digital and other cutting edge technologies, the Department will be able to provide all hazards alerts and warnings to the greatest number of people. This includes persons with disabilities and individuals for whom English is a second language.

For example, we have been conducting a Digital Emergency Alert System pilot project in the National Capital Region with the Association of Public Television Stations. This pilot has successfully demonstrated how the capabilities of America's public broadcasters can be utilized to dramatically enhance our ability to provide the American people with critical, and lifesaving, information. Significantly, through the voluntary cooperation and full participation of public and commercial broad-

casters, satellite radio, the cellular telephone industry, technology developers, pager service providers, cable operators, and others, we have successfully demonstrated an ability to transmit a variety of alert and warning messages via digital television and satellite to a full range of retransmission media using a common alerting protocol. We are especially pleased that NOAA and the FCC have been full partners with us in this Digital Alert and Warning System pilot and have recently added the Department of Justice and The Weather Channel to our list of pilot participants.

Building upon the success of our Digital EAS pilot we have begun a second phase expansion in which we will replicate our experience in the National Capitol Region at other sites across the country using public television's existing digital infrastructure. Our intent in this second phase of the Digital EAS pilot is to demonstrate a national capability, identify technological challenges, and develop a nationwide implementation plan.

Because there is no single solution set available that can provide for all of the alert and warning systems requirements for Federal, State and local users, our IPAWS uses a "system of systems" approach and does not totally rely upon the digital infrastructure of Public Television. Working in partnership with NOAA we are including under the IPAWS umbrella a Geo-Targeted Alerting System (GTAS), which uses reverse 911 technology, to demonstrate and test the ability to provide targeted warning down to the individual household or business. This GTAS pilot will be conducted in the National Capital Region with the goal of expanding alert and warning capabilities to include plume hazard warning.

Since the beginning of the IPAWS initiative our focus has been demonstrating and developing the best technologies available without regard to the emergency message content. Moreover, because we are incorporating common alerting protocols and using digital technology we have better positioned a national alert and warning system to be an all hazards system. In this regard, the recent passage of the Intelligence Reform Bill directed the Department to work with the National Association of State Chief Information Officers (NASCIO) to demonstrate an Amber Alert like web portal. We have been working with NASCIO to finalize a Cooperative Agreement that will help us add another powerful dimension to the IPAWS. This effort will also build upon the successes and lessons learned that the Department of Justice has demonstrated in not only partnering with the wireless community to provide missing child alerts, but also providing an effective web based portal solution for its Amber Alert program.

A primary mission of our office remains assuring the ability of the President, and senior government leaders, to address the Nation under the most extreme circumstances. This year, we are upgrading the Primary Entry Point (PEP) system from its current ground-based dial up capability to a satellite distribution system. We will also be expanding the number of PEP broadcast stations so that each state and territory will have a direct satellite receive capability. These critical upgrades will ensure the survivability of radio broadcast systems in the event of a catastrophic incident. Moreover, by leveraging public-private partnerships with satellite and public radio, we are able to significantly enhance the Emergency Alert System without a major investment in new infrastructure.

We recognize that there is no single solution set that will meet everyone's alert and warning requirements, that is why FEMA, IAIP and the Department has teamed up with NOAA, the FCC, DOJ and the private sector to find the most appropriate interoperable solutions to develop the Integrated Public Alert and Warning System approach. We believe that IPAWS, using digital technology in combination with upgraded Primary Entry Point EAS capabilities, will provide Federal, state and local emergency managers and leaders with the tools they need to alert America about both man-made and natural disasters. At the same time we are aware of the concerns of our state partners who have invested in their own alert and warning systems. With that in mind, IPAWS is intended to be fully interoperable with those systems using common alerting protocols. As we proceed, we will continue to reach out to state and local users to integrate a national alert and warning system into their existing capabilities which will result in significant improvements in public awareness during hazardous events.

Because our IPAWS framework is based upon the premise of providing alert and warning messaging in a coordinated manner, over as many platforms as possible, to ensure the widest dissemination and public receive capabilities, the Department of Homeland Security is also providing funds to NOAA for system upgrades to the NOAA Weather Radio All Hazards network. In addition, in partnership with the Department of Education and the Department of Commerce, IAIP is funding a pilot program to purchase NOAA Weather Radio All Hazards receivers for certain public schools across the Nation. We are also reaching out to the many stakeholders and alert and warning systems users through a series of IPAWS seminars. Our first

seminar was conducted in April and brought together Federal, state, local, and private sector groups to begin a dialog with us on IPAWS. Significantly, the seminar attendees included representatives from the disabled community who told us about the challenges they face with regard to alert and warning. We are continuing that dialogue and working to incorporate their concerns with IPAWS solutions. The Department, and our Federal partners, will continue these IPAWS outreach seminars as a means to educate the public and ensure we are adding needed alert and warning capabilities—not adding another burden on those who use and depend upon such systems to save lives and protect property.

We are pleased that the FCC, last year, issued a Notice of Proposed Rulemaking with regard to the Emergency Alert System. We believe that the FCC's efforts in this matter will help us strengthen and improve alert and warning for the general public and we look forward to continuing our close cooperation with the Commission as they move toward a decision.

Finally, Mr. Chairman, the Task Force on Effective Warning that I mentioned at the outset of my remarks is working to develop a national alert and warning policy that recognizes the IPAWS solution. Moreover, with the help of the Department of the Interior's USGS, and other emergency message originators in the Federal Government, we will be able to build upon their experiences and capabilities to incorporate tsunami, earthquake and other warnings to the public into a national all hazards IPAWS.

Mr. Chairman these are just some examples of how FEMA and the Department of Homeland Security has taken seriously its responsibility to ensure the quick and accurate dissemination of alert and warning information to our homeland security partners and the American public.

Thank you again for the invitation to speak, for your support of the Department's mission, and for your interest in effective alert and warning systems. I will be pleased to answer any questions you may have.

Senator DEMINT. Thank you, Mr. Hoover. We'll save our questions until the panel has completed their statements.

Mr. Moran?

**STATEMENT OF KENNETH MORAN, ACTING DIRECTOR, OFFICE OF HOMELAND SECURITY, ENFORCEMENT BUREAU, FEDERAL COMMUNICATIONS COMMISSION (FCC)**

Mr. MORAN. Good morning, Mr. Chairman and Senator Nelson. I'm Kenneth Moran, Acting Director of the Enforcement Bureau's Office of Homeland Security at the Federal Communications Commission. I welcome this opportunity to appear before you to discuss the FCC's activities regarding the Emergency Alert System.

For over 50 years, the United States has had a mechanism in place to allow the President to communicate with the public in the event of a national emergency. Currently, that mechanism is the Emergency Alert System, or EAS.

Under our EAS rules, radio, television, and cable systems are required to deliver Presidential-level emergency messages. In addition, EAS has been used on a voluntary basis for delivery of State and local emergency messages.

Today, we face new homeland security threats and challenges, and the Commission is acutely aware of the importance to the American public of timely and effective emergency warnings. In addition, in recent years, there have been many important advancements in communications technologies that may afford opportunities for improving EAS.

As a result, EAS has been the subject of an extensive examination to ensure that we do our part to contribute to an efficient and up-to-date public alert and warning system. The Commission is conducting a rulemaking proceeding to consider whether EAS is the most effective way to warn the American public of an emer-

gency; and, if not, how the system can be improved. Because this proceeding is ongoing, my comments in this hearing are limited to the record that has developed so far.

In its rulemaking proceeding, the Commission raised broad questions regarding whether EAS's capabilities are consistent with the Commission's mission to ensure that the public warning system takes full advantage of current and emerging technologies. Specifically, the Commission sought comment on whether EAS should be adapted or redesigned to take advantage of digital, satellite, and other wireless technologies.

What we've learned is that most parties advocate improving the existing system rather than completely redesigning it. The Commission also raised the issue of whether the voluntary nature of EAS at the state and local levels remains appropriate in today's world. Some of the commentors argue that it should be mandatory; others have suggested that voluntary participation by media to deliver state and local emergency messages has proven to be effective and should be allowed to continue.

We also asked comment on a number of other issues, such as the respective roles of the Federal departments and agencies involved in the implementation of EAS, the security of the public warning system, improvements to the testing of the program, how a public warning system can most effectively provide emergency warnings to the disabled community and to those for whom English is a second language. Indeed, a key focus of our work is how to reach each and every citizen with the right emergency-alert warning information at the right time. The FCC has, and will continue to, coordinate with the Department of Homeland Security, FEMA, NOAA, and others as we examine these issues. We anticipate that our Federal partners will continue to be active participants in our proceeding, and we also expect to continue to receive valuable input from interested individuals, state and local emergency management agencies, tribal governments, and various elements of the communications sector.

And we look forward to working with the Congress, Federal, state, and local emergency managers, industry, and the public to ensure that we can provide an effective warning system to the American people.

I thank you, Mr. Chairman, for the opportunity to appear. This concludes my testimony. I'd be happy to answer any questions that you or the other Members may have.

Thank you.

[The prepared statement of Mr. Moran follows:]

PREPARED STATEMENT OF KENNETH MORAN, ACTING DIRECTOR, OFFICE OF HOMELAND SECURITY ENFORCEMENT BUREAU, FEDERAL COMMUNICATIONS COMMISSION (FCC)

**Executive Summary**

Since the Cold War era, the United States has had a mechanism in place for the President of the United States to communicate with the public in the event of a national emergency. Under the current Emergency Alert System (EAS), all analog broadcast radio, television, and cable systems are required to deliver a Presidential-level activation of EAS, but their use of EAS in response to State and local emergencies, while encouraged, is voluntary.

In light of today's homeland security threats, the Federal Communications Commission (Commission) remains acutely aware of the importance of timely and effec-

tive warnings. In addition, there are exciting changes in our communications media that may allow for improvements in our warning systems. As a result of these changes, EAS has recently been the subject of much examination. To ensure that the Commission does its part to contribute to an efficient and technologically current public alert and warning system, the Commission is conducting a rulemaking proceeding to consider whether the current EAS is the most effective way to warn the American public of an emergency and, if not, how the system can be improved.

As part of the current EAS proceeding, the Commission raised broad questions about whether the technical capabilities of EAS are consistent with the Commission's mission to ensure that public warning systems take full advantage of current and emerging technologies, particularly digital broadcast and wireless telecommunications media. For instance, the Commission noted that some parties argue that the purely voluntary nature of EAS at the state and local level results in an inconsistent application of EAS as an effective component of an overall public alert and warning system. The Commission also is considering issues such as what the respective roles of the Federal Government departments and agencies involved in the implementation of EAS should be, how the delivery pipeline for public warning can be made more secure and how it can be tested, how both emergency managers and the public can use and respond to a public warning system in the most effective manner, and how a public warning system can most effectively provide emergency warnings to the disabled community and those for whom English is a second language. Indeed, a key focus of the Commission's inquiry is how to reach each and every citizen.

The Commission has coordinated closely with the Department of Homeland Security (DHS) and its component, the Federal Emergency Management Agency (FEMA), and with the National Oceanic and Atmospheric Administration (NOAA) and its component, the National Weather Service (NWS). The Commission values these agencies' continued participation in our review of EAS.

The Commission looks forward to working with Congress, our colleagues at other Federal, state and tribal agencies, and the public to ensure that it can provide such a warning system to our citizens.

**Introduction**

Mr. Chairman and Members of the Subcommittee:

Good morning. I am Kenneth Moran, Acting Director of the Federal Communications Commission (Commission) Enforcement Bureau's Office of Homeland Security. I welcome this opportunity to appear before you to discuss the Emergency Alert System, or EAS.

The Commission is well aware that an effective public alert and warning system is an essential element of emergency preparedness, and that such a system is impossible without effective communication and coordination within the Federal Government, as well as with the active participation of the states and the private sector. Accordingly, the Commission has been working with other Federal agencies, state governments, and industry to ensure that the American public is provided with a robust, efficient, and technologically current alert and warning system.

**Background**

The forerunner of our current Emergency Alert System originated in the early days of the Cold War when President Truman established the "CONELRAD " system as a means to warn the public of an imminent attack. Since that time, CONELRAD has given way to the Emergency Broadcast System, which in 1994 was replaced by EAS. From the early CONELRAD days to the present, the Commission has played a critical role in ensuring that the President of the United States would be able to communicate with the American public in the event of a national emergency. Today's EAS uses analog radio and television broadcast stations, as well as wired and wireless cable systems, to deliver a national Presidential message. When activated, EAS would override all other broadcasts or cable transmissions, national and local, to deliver an audio Presidential message. This system is mandatory at the national level, but is also available on a voluntary basis for states and localities to deliver local emergency notifications.

The Commission, in conjunction with the Federal Emergency Management Agency (FEMA) and the National Weather Service (NWS), implements EAS at the Federal level. Our respective roles currently are based on a 1981 Memorandum of Understanding between FEMA, NWS, and the Commission, on a 1984 Executive Order, and on a 1995 Presidential Statement of Requirements.

The Commission's EAS rules are focused on national activation, and the delivery of a Presidential message. The Commission's rules prescribe: (1) technical standards for EAS; (2) procedures for radio and television broadcast stations and cable systems

to follow in the event EAS is activated; and (3) EAS testing protocols. Under the rules, national activation of EAS for a Presidential message is designed to provide the President the capability to transmit from any location at any time within 10 minutes of the system's activation, and would take priority over any other message and preempt other messages in progress. Currently, only analog radio and television stations, and wired and wireless cable television systems, are required to implement the national EAS. Other systems, such as digital television (DTV), Direct Broadcast Satellite television (DBS), Low Earth Orbit (LEO) satellite systems, paging, Satellite Digital Audio Radio Service (SDARS), and In-Band-On-Channel Digital Audio Broadcasting (IBOC DAB) are currently not required to participate in EAS.

The decision to activate the national-level EAS rests solely with the President. FEMA acts as the White House's executive agent for the development, operations, and maintenance of the national level EAS and is responsible for implementation of the national level activation of EAS, as well as EAS tests and exercises.

EAS is essentially a hierarchical distribution system. FEMA has designated 34 radio broadcast stations as Primary Entry Point (PEP) stations. At the request of the President, FEMA would distribute the "Presidential Level" messages to these PEP stations. The PEP stations are monitored in turn by other stations in the hierarchical chain. Commission rules require broadcast stations and cable systems to monitor at least two of the EAS sources for Presidential alerts that are specified in their state EAS plans. Initiation of an EAS message, whether at the national, state, or local level, is accomplished via dedicated EAS equipment. The EAS equipment provides a method for automatic interruption of regular programming and is capable of providing warnings in the primary language that is used by the station or cable system.

Along with its primary role as a national public warning system, EAS—and other emergency notification mechanisms—are part of an overall public alert and warning system, over which FEMA exercises jurisdiction. EAS use, as part of such a public warning system at the state and local levels, while encouraged, is voluntary. Nevertheless, the public receives most of its alert and warning information through the broadcasters' and cable systems' voluntary activations of the EAS system on behalf of state and local emergency managers.

**Current Issues and the Commission's Rulemaking Proceeding**

As noted above, the public relies heavily on EAS for emergency information. EAS therefore serves a critical purpose, but it currently only applies to analog radio and television stations, and wired and wireless cable television systems. In August 2004, the Commission began a rulemaking proceeding to review whether we need to either update EAS or replace it with a more comprehensive and effective warning system.

In initiating its rulemaking, the Commission encouraged commenters to consider recommendations from two public/private partnerships that have studied EAS issues extensively: the Media Security and Reliability Council (MSRC), an industry-led Federal Advisory Committee comprised of representatives from the radio, television, multi-channel video, public safety, and disabilities communities, and the Partnership for Public Warning (PPW), a not-for-profit, public/private partnership that was incorporated with the goal of promoting and enhancing effective, integrated dissemination of public warnings.

The Commission has received comments from numerous interested individuals, Federal entities, State and local emergency planning organizations, and various sectors of the telecommunications industries. We have coordinated with DHS and its component, FEMA, and with the Department of Commerce and its component, the National Oceanic and Atmospheric Administration's (NOAA) National Weather Service, and we will continue to do so.

The overarching question addressed in the proceeding is whether EAS in its present form is the most effective mechanism for warning the American public of an emergency, and, if not, how EAS can be improved. Most of the parties who commented agree that our warning system should be improved. Most—including MSRC and PPW—also advocate upgrading, rather than replacing EAS, to take advantage of the existing EAS infrastructure.

The Commission's rulemaking proceeding addresses a number of specific and timely issues. For instance, the Commission noted that some parties argue that the purely voluntary nature of EAS at the state and local level results in an inconsistent application of EAS as an effective component of an overall public alert and warning system. To address these arguments, the Commission is examining whether permissive state and local EAS participation remains appropriate today, and whether uniform national guidelines should apply to state and local EAS implementation. Some parties who commented on this issue support continuing voluntary participation, at least for the present, while the Commission considers broader changes

to EAS. Some parties also stated that participation, though voluntary, is widespread. These parties generally support continuing the voluntary nature of EAS

The Commission's Notice of Proposed Rulemaking (NPRM) initiating the open proceeding focused on the fact that EAS is currently mandated only for analog television and radio, and for cable systems, which represent an increasingly smaller part of our information sources. The Commission is considering whether and how EAS obligations should be extended to services not currently covered—*e.g.,* digital television and radio, and satellite radio and television. Many commenters support the Commission's efforts to extend the EAS rules to digital broadcasters.

The NPRM also asked questions about whether the technical capabilities of EAS can or should be applied to other communications platforms. Along with digital broadcast, new digital wireless technologies, including cellular telephony and personal digital assistants, are rapidly redefining the communications landscape, making available to the public warning technologies that are far more flexible and effective than the analog broadcast mechanism currently employed by EAS. The Commission is considering whether there should be an effort to use such technologies to form a comprehensive national public warning system capable of reaching virtually everyone all the time by combining EAS with alternative public alert and warning systems. We received a number of comments about methods, such as cell phone broadcasting, that could expand the reach of our warning systems in the future. In their comments, DHS and FEMA also noted that they are investigating new technologies for this purpose.

The Commission also is examining security and reliability issues relevant to EAS and on the important question of how best to supply an effective public warning system to the disabled community and non-English speakers. The Commission is also considering the role of various Federal Government departments and agencies, as well as local authorities, in implementing EAS.

In addition, the Commission is involved in other initiatives, beyond its rulemaking proceeding, to address the effectiveness of our Nation's warning systems. For instance, the Commission is participating in the Task Force on Effective Warnings Materials, a group of Federal departments and agencies that has been assembled to examine existing and planned disaster warning and communications systems, and to make recommendations to ensure that these systems are effective. We will continue to share our expertise and views, and to seek the expertise and views of others, on these important issues.

**Conclusion**

The Commission looks forward to working with Congress, our colleagues at other Federal, state, and tribal agencies, and the public to ensure that we can provide an effective and technologically advanced warning system to our citizens. The Commission also is aware that the Congress is taking an active interest in the issue of public alert and warning, and stands ready to provide whatever technical assistance that the Congress would find helpful in this regard.

Senator DEMINT. Thank you.

Our Chairman has joined us. Mr. Chairman, we're hearing from FEMA, the FCC, and getting ready to hear from Mr. Paese, from NOAA. They are giving us an update on the development of a national all-hazards alert system.

So, Mr. Paese? Have I got that name anywhere close to being right?

Mr. PAESE. Perfect.

Senator DEMINT. OK.

## STATEMENT OF MARK PAESE, DIRECTOR, MAINTENANCE, LOGISTICS AND ACQUISITION DIVISION, NATIONAL WEATHER SERVICE, NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION (NOAA)

Mr. PAESE. Thank you, Mr. Chairman and members of the Committee.

I am Mark Paese, Director of Maintenance, Logistics, and Acquisition for the National Weather Service at NOAA. I am pleased to be here today to discuss NOAA Weather Radio, All Hazards.

Known as "The Voice of the National Weather Service," NOAA Weather Radio, All Hazards, is provided as a public service. The NOAA Weather Radio All Hazards Network includes 935 transmitters covering all 50 states, adjacent coastal waters, Puerto Rico, the U.S. Virgin Islands, and U.S. Pacific territories. The nationwide network of radio stations provides coverage to over 97 percent of the U.S. population. This extensive system of radio transmitters allows the National Weather Service to transmit routine observations and forecasts, as well as alerts and warnings of severe weather and other hazardous information, 24 hours a day, 7 days a week.

In June 2004, NOAA and the Department of Homeland Security signed an agreement providing DHS the capability to send critical all-hazards alerts and warnings through the NOAA Weather Radio Network. Now NOAA Weather Radio broadcasts warnings and posts that information for all types of hazards—natural, such as earthquakes, tsunamis, hurricanes, and volcanic activity; man-made, such as chemical releases or oil spills; and terrorist alerts. NWS warnings are carefully developed to ensure critical information is conveyed as directly as possible. Each warning contains several components that are based on discussions with users, including the private sector, emergency managers, and the public. We also work with sociologists and others to ensure the information in our message is worded as clearly as possible for the public to understand what to do.

While the current network works well, NOAA Weather Radio has some challenges. We need to ensure a fully-functioning network through continued maintenance, upgrading older and solid-state transmitters, installing backup power at locations without this capability, and provide the connectivity between alert sources and the transmitter. Existing dissemination systems were developed to meet specific user requirements for information. Warning systems must look toward the future and include graphical forms of information readily available through advanced technology, such as cell phones and PDAs.

Future systems should also improve on existing geo-targeting to be able to reach people where they are—work, home, or on the move—and reduce unnecessary warnings to people who are not in hazardous zones.

Recognizing the need for a national all-hazards alert system, Department of Homeland Security and NOAA serve as Co-Chairs of the White House Task Force on Effective Warnings. The effort was chartered by the Office of Science Technology Policy to develop a government-wide plan for an integrated Public Alert and Warning System, or IPAWS. There will be many—there are many warning systems across the country, and an integrated system of systems will be far better than any one system.

In Fiscal Year 2004, NOAA began developing a capability to reduce the time it takes for an emergency manager to input a hazard warning into NOAA Weather Radio and reduce the possibility of any transcription errors. This system, known as HazCollect, will reduce the amount of time it takes to input a message into the system from 7 minutes to less than 2 minutes. This capability is expected to be fully operational in Fiscal Year 2006.

NOAA's vision for the future is to ensure access and delivery of environmental warnings, forecasts, and information to every person in the United States. To achieve this vision, it is essential to use emerging technologies to make warnings and information available via convenient methods and formats to as many individuals as possible. We are working with the private sector to make this happen. Government and the emergency community must work together to develop an integrated Public Alert and Warning System adaptable to change.

Standards and protocols such as Common Alerting Protocol, or CAP, recently agreed upon by the emergency-management community, is one example of how the collaboration of the emergency management community and the government has increased interoperability.

The Department of Homeland Security, in partnership with NOAA and the Department of Education, is funding a pilot program to develop NOAA Weather Radios at public schools in the top urban-area security initiatives in two rural states.

NOAA Weather Radio is a proven technology. It works, and it saves lives. Seven weeks ago, in Endicott, New York, the Principal at Charles F. Johnson Elementary School received a severe-thunderstorm warning on their school NOAA Weather Radio. He implemented his school safety plan and moved the 340 students and faculty out of harm's way. Twenty minutes later, 70-mile-an-hour winds ripped the roof off the kindergarten wing and devastated the building.

In conclusion, NOAA Weather Radio is a proven dissemination network that has saved lives. We will continue to work with other agencies to achieve the vision to reach every person in the United States.

I would be happy to answer any questions.

[The prepared statement of Mr. Paese follows:]

PREPARED STATEMENT OF MARK PAESE, DIRECTOR, MAINTENANCE, LOGISTICS AND ACQUISITION DIVISION, NATIONAL WEATHER SERVICE, NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION (NOAA)

Mr. Chairman and members of the Committee, I am Mark Paese, Director of Maintenance, Logistics, and Acquisition Services for the National Weather Service (NWS), of the National Oceanic and Atmospheric Administration (NOAA) within the Department of Commerce. I am pleased to be here today to discuss NOAA Weather Radio All Hazards (NWR). I will outline how our system currently works and our vision for the future.

**Introduction and Background**

Known as the "Voice of the National Weather Service," NOAA Weather Radio All Hazards is provided as a public service. The NOAA Weather Radio All Hazards (NWR) network includes 935 transmitters, covering all 50 states, adjacent coastal waters, Puerto Rico, the U.S. Virgin Islands, and the U.S. Pacific Territories. The NWR nationwide network of radio stations provides coverage to over 97 percent of the population. This extensive system of radio transmitters allows the National Weather Service to transmit routine programming containing observations and forecasts, with this routine programming interrupted to broadcast alerts and warnings of severe weather and other hazardous information 24 hours a day. Each transmitter is automatically fed information from the local NWS weather office typically via telephone lines, while some more remote locations use microwave transmissions. It takes only seconds from when the forecaster hits the send button until the message is transmitted on the network. NWR requires a specific radio receiver or scanner, readily available at most electronic stores, capable of receiving the broadcast.

This NWS direct broadcast includes special codes identifying alerts and warnings, with many receivers equipped to monitor these codes.

NWR receivers should be as common as smoke detectors especially given their capability to wake people in the middle of the night when hazardous conditions threaten. In addition to the traditional weather radio that many are familiar with, NOAA Weather Radio All Hazards receivers can be integrated into devices to turn on alarms, lights, bed shakers, and other equipment especially useful for the hearing impaired community and those with special needs.

Agreements with local, State, and Federal emergency managers and first responders, and working with the Federal Communications Commission's (FCC's) Emergency Alert System, allow NWR to act as a direct, official source for comprehensive weather and emergency information—an "all hazards" warning system. In June 2004, NOAA and the Department of Homeland Security signed an agreement allowing DHS to send critical all-hazards alerts and warnings directly through the NOAA Weather Radio All Hazards network, further leveraging NWR as a backbone of a national emergency alert and warning system. With this agreement in place, NWR is the only Federal Government warning system that can be targeted to specific areas to deliver a message from the President. NOAA Weather Radio All Hazards also broadcasts warning and post-event information for all types of hazards—both natural, such as earthquakes, tsunamis, hurricanes, and volcanic activity, and man made, such as chemical releases or oil spills. Many emergency dispatch centers, institutional (day care, elder care, hospitals, schools, etc), building and manufacturing security operations centers monitor NWR for emergency warning information as a public safety tool.

NWS warnings are carefully developed to ensure critical information is conveyed as directly as possible, regardless of the transmission on NWR or any of the other dissemination systems. Each warning contains several components, which are included based on NWS discussions with users, including private sector, emergency managers, and the public. We also worked with sociologists and others to ensure the information in our messages is worded as clearly as possible for the public to understand what to do. The messages include appropriate "call to action" statements advising people of actions to take (seek shelter indoors, avoid crossing high water, etc.). The messages also contain critical event and geographic information for other dissemination and computer systems to decode and retransmit. For example, the Emergency Alert System (EAS) operated under FCC rules is automatically activated by NWR broadcasts of warnings.

**Upcoming Challenges for NOAA Weather Radio All Hazards**

While our current network works well, NWR has some challenges. We need to ensure a fully functioning network through continued maintenance, upgrading older solid state transmitters, public education and awareness about the capabilities of the network, installing backup power at locations without this capability to ensure continued service when commercial power fails, and upgrading the telecommunication feed from the NWS office to the transmitter.

The number of NWR transmitters has more than doubled in the past decade. Today, 935 transmitters are in operation, with three more scheduled to come on line by the end of the September. NWR intends to upgrade older transmitters to new technology standards. These upgrades to 400 transmitters will be completed by FY 2011. We will be increasing coverage to 100 percent for areas of the Nation particularly vulnerable to severe weather and tornadoes, such as tornado alley. Current projections call for meeting this goal in 2007. We also plan to provide backup power to all NWR stations by 2012, which includes about 440 currently without that capability. We have a plan to provide a more reliable and robust communication feed directly to the transmitters. Converting to this new process should be complete in FY 2009.

**Next Generation Warning System**

Existing dissemination systems were developed to meet user requirements for information. Any future warning system must go beyond direct radio broadcasts and include visual forms of information readily available through advancing technology (*e.g.,* cell phones, Personal Digital Assistants, etc). Future systems should also improve on existing geo-targeting/referencing to be able to reach people where they are—home, work, or on the move—and to reduce warnings to people who are not in the hazardous zones.

Hazardous weather and water forecasts, warnings, and other hazards information are delivered as quickly as possible using "push" and "pull" dissemination technologies, which respectively send information and allow information to be retrieved. "Push" occurs when messages and information are broadcast or sent to the recipient

(e.g. a radio is push technology). "Pull" technology includes mechanisms in which information is transmitted in response to a request from a user (*e.g.,* using Internet browsers to request information).

Push (send) capabilities distribute scheduled and unscheduled warnings, forecasts, and information using a predetermined priority. Warnings are given the highest priority. For example, NOAA Weather Radio All Hazards is a "push" technology; it provides 24-hour access to weather information and other all-hazards information. NWR is one component of the existing NWS dissemination infrastructure, which also includes NOAA Weather Wire Service, Emergency Managers Weather Information Network or EMWIN, Family of Services, and NOAAPort. Pull (retrieve) capabilities make warnings, forecasts, and information available for people to acquire as needed. The Internet is our primary use of a "pull" technology; it enables users to retrieve environmental information as needed from NOAA web pages and other locations.

Recognizing the rapid advances in information technologies, the Department of Homeland Security and NOAA co-chair an effort to develop a government-wide plan for the Integrated Public Alert and Warning System (IPAWS). The government's ability to effectively warn the public of danger will be greatly improved by implementing IPAWS. Public safety is a fundamental responsibility of Federal, state and local governments. Public warnings save lives by informing, reducing fear, recommending action, and assisting emergency managers. The Administration is formulating an overall plan for emergency broadcasts and warning systems. There are many warning systems in place across the country, ranging from local phone warning capability, local sirens, paging systems, Internet notification, to national level-warning programs, including the NOAA Weather Radio All Hazards. Each of these systems by themselves can reach the public directly, but each has limitations. An integrated system employing all of these capabilities will be far better than any single system.

In FY 2004, NOAA began developing a capability to reduce the time it takes for an emergency manager to input a hazard warning into NOAA Weather Radio All Hazards and reduce the possibility of transcription errors. This system, known as HazCollect, will reduce the amount of time it takes to input a message into the system—from 7 minutes to less than 2 minutes. This capability will allow emergency managers direct access to Emergency Alert System (EAS) via NOAA Weather Radio All Hazards, and is expected to be fully operational in FY 2006.

**A Vision for the Future**

*Our Vision—Reach each person in the Nation.* NOAA's vision is to ensure access and delivery of environmental warnings, forecasts, and information to every person in the United States. This dissemination system should provide climate, water, weather and other hazard information the public wants, when they want it, where they want it, how they want it, and should ensure persons at risk receive timely alerts. Warnings do not become effective until those in harm's way hear the warning and take appropriate action. Advanced, universally accessible dissemination technologies are necessary to deliver environmental information for the protection of life and property. Universal access depends upon partnerships within communities to increase awareness and coverage.

To achieve this vision, it is essential to use emerging technologies to improve communication performance measured by operational availability, latency, cost effectiveness, and most importantly, customer satisfaction. We need to make warnings and information available, via convenient methods and formats (e.g., industry standards such as GIS, XML and Real Simple Syndication (RSS)), to as many individuals as possible. We are working now to make this happen.

The emergency information community and the government must work together to develop a dissemination program that is integrated and adaptable to change. The Common Alerting Protocol (CAP), recently agreed upon by the emergency management community, is one example of how the collaboration of the emergency management community and the government has increased the effectiveness of the alerting system. HazCollect will use the CAP format for emergency messages.

To be most effective, emergency information must penetrate all technologies—radio, TV, satellite radio, satellite TV, fixed telephony, mobile telephony and the Internet, including voice over Internet provider (VOIP), in addition to system-specific receivers like NWR—and recognize the limitations of each. No single technology or system will reach all end-users. The most critical information must be "pushed" to the end users.

We must account for a broad spectrum of users, from those who want simple access to basic information to those who want customized access in order to extract

information to meet their needs and, finally, those who want to download data in bulk.

Current and future technologies must be leveraged to combine common functions into a streamlined dissemination process. Because many push systems share common features, current and future technology advances will facilitate merging the functionality of the various systems while fulfilling their individual requirements. A properly planned network will yield reliable, and cost effective services.

The NWS depends on close working relationships with media and vendor groups to disseminate NWS information, especially warnings and forecasts, and must consider the essential role of its partners in dissemination. We will work more closely with industry leaders so NWS will be able to reach the public through such target technologies as satellite radio, satellite television, cable television, broadcast television, mobile/cellular telephony, fixed telephony (land lines), commercial radio, and the Internet (including VOIP).

Flexibility must be "built in" to formats, standards and protocols used to disseminate information. NWS and the entire all-hazards community should adopt policies to put themselves in a position to efficiently modify the formats and protocols used for dissemination as industry standards evolve and as new technologies become available. For example, the Internet text format known as Extensible Markup Language (XML) is necessary to support more sophisticated and automated data discovery, selection and retrieval mechanisms. XML is a simple, very flexible text format originally designed to meet the challenges of large-scale electronic publishing. XML is also playing an increasingly important role in the exchange of a wide variety of data on the Internet and elsewhere. NWS will also need to respond to the growing popularity of GIS formats.

We need to improve performance to keep pace with the need for more data and information in various formats by maintaining adequate processing speed, appropriate latency, and cost effectiveness. As science and technology continue to advance, more data sets, and more information will become available. Data compression techniques will allow more information to be transmitted by fully exploiting the communications infrastructure.

Finally, we need to investigate emerging technologies to fulfill dissemination requirements beyond the next few years. Technologies such as software-defined radio (SDR)/cognitive radio would allow the user more precision and flexibility in deciding which information to hear. Cognitive radio knows where it is, what services are available, and what services interest the user. WiFi (wireless fidelity) and voice over wireless LAN (VoWLAN) provide an expanded opportunity to reach a more mobile public.

**Conclusion**

NOAA Weather Radio All Hazards is a proven dissemination network that has saved lives. We will continue to exploit our existing technology. However, technological advances will continue to drive how we can best communicate critical information to an ever more mobile and technology equipped public. It is our responsibility to ensure critical emergency information is available and can reach the people as easily and conveniently as possible. We will continue to work to achieve our vision to reach every person in our great Nation.

Senator DEMINT. Thank you.

Mr. Chairman, would you like to make a statement?

## STATEMENT OF HON. TED STEVENS, U.S. SENATOR FROM ALASKA

The CHAIRMAN. Well, thank you very much, Mr. Chairman.

I've come over to really put in the record the fact that, at my request, we've put $10 million in the budget now, for 2 years, and there's $5 million in the bills that are pending now, to pursue this effort. I hope that it will—I think that money also includes a pilot project on using the NOAA Weather Radios, and they're being tried out in the offshore states, I believe. But I do hope that we can find a way to really bring about the total coordination that you've mentioned.

And my basic question is, Is this money enough? Are we going to be able to get this job done with the money we've got now and

appropriated in the past? Who wants to answer that? It went to Homeland Security, so why don't the Homeland Security people answer?

Mr. HOOVER. Thank you, Mr. Chairman.

You are correct, in the Fiscal Year 2004 and 2005 budgets, the Congress appropriated $10 million in each year to the Department of Homeland Security. Those funds went to IAIP, the Information Analysis and Infrastructure Protection directorate. We have coordinated with IAIP over the last 2 years, the last two fiscal years, and, in fact, have coordinated our efforts with regard to the alert and warning upgrades.

As part of the funding that you've mentioned, we have provided funds for the upgrade of the NOAA All–Hazards Radio Network. We have provided funds for providing radios, NOAA Weather Radios, to schools, as Mark had just previously testified to. And the monies that we are using is really—the 10 million this year and last year—are funds that are for that IPAWS initiative, that, both within the Department, we're coordinated on, and, as well, across the government, that we're coordinated on to move forward to bring the next-generation alert and warning system into being.

The CHAIRMAN. At a recent meeting I attended, I was told that the—really, the key to this effort is software. Are you developing software so there will be, really, a continuity throughout all systems using the same software?

Mr. HOOVER. There is some software development that's going on in the background, and I am not that technical to be able to tell you all the software pieces of it. And the key, I think, is—as you're alluding to—is the integration piece. The technology's out there. And I think today, in the next panel, you'll see a demonstration from—what we're doing with the digital emergency alert system. The technology is there. The challenge is the integration of all of those systems so that we can reach all of the American public at the right time with the right information.

The CHAIRMAN. Well, I'm sorry, Mr. Chairman, I have to go to another meeting.

But I don't think you quite answered my question about money. Is that five million going to be sufficient to complete this initial phase of this integration?

Mr. HOOVER. We believe that—if that's in the—if the Congress is going to give us $5 million, Mr. Chairman, that will be sufficient for us to continue to move forward with the IPAWS program.

The CHAIRMAN. What is your time frame? What is the target date for initiating the system?

Mr. HOOVER. Mr. Chairman, we're actually in the process now of rolling out a second phase of the digital pilot that we're working with, APTS, to demonstrate a nationwide capability for distribution, to identify some additional technological issues that are out there, and then develop a nationwide implementation plan. And we're moving forward with that right now.

The CHAIRMAN. You still haven't answered me. What—do you have a target date?

Mr. HOOVER. I can't give you a target date, Mr. Chairman, in terms of when the system actually will be in place and operational. I can tell you that, as we move forward—and I would expect, by

the end of next fiscal year, we would be in a position to have the basics of the backbone system in place so that we can move forward to have a full implementation.

The CHAIRMAN. Maybe time-sensitive about that. Do you know, my state has more natural disasters than any part of the United States? Hawaii comes second. Now, the two of us from the Pacific are very concerned about this, and we think there ought to be a date when people can understand this system will be in place.

Mr. HOOVER. Well——

The CHAIRMAN. Now, when will you be able to answer the question of, When will the system be in place and operable?

Mr. HOOVER. Well, Mr. Chairman, it's important to recognize that there already is a system in place to warn the public for emergencies, and that is the Emergency Alert System, and it is used every day. What we're doing now is taking that one step further and implementing—using new digital technologies to be able to reach out to more people, more of the time.

The CHAIRMAN. That relies on——

Mr. HOOVER. So, we do have a system in place.

The CHAIRMAN.—just on radio, doesn't it?

Mr. HOOVER. Yes, sir. I mean, the foundation of the EAS system is based on the broadcasters and the broadcasters' participation.

The CHAIRMAN. That was a wonderful system for its time, but I don't know many people that carry around radios in their pocket any longer. They're carrying cell phones, they've carrying BlackBerrys, they're carrying all sorts of devices for communication, and we need to get in touch with the future on this system. When is that integration date?

Mr. HOOVER. Mr. Chairman, I can't give you an exact date. I can tell you that by the end of next year we will be well along the way to fully deploying an Integrated Public Alert and Warning System.

The CHAIRMAN. OK. Then, Mr. Chairman, you can tune in the same station next year, I'll ask you the same question next year.

Mr. HOOVER. Thank you, sir.

The CHAIRMAN. Thank you very much.

Senator DEMINT. Thank you, Mr. Chairman.

As you probably understand, we might need to come up with a date at——

Mr. HOOVER. Yes, sir.

Senator DEMINT.—this point.

[Laughter.]

Senator DEMINT. And, Mr. Hoover, my respect——

Mr. HOOVER. Got that loud and clear, Mr. Chairman.

[Laughter.]

Senator DEMINT. Good, I'm glad we—we're understanding the same message here.

Mr. Hoover, my respect for you has gone way up. I've never heard anyone in a Federal agency say they have enough money, so I appreciate——

[Laughter.]

Senator DEMINT.—us starting that way.

Let me start with a couple of questions, and then I'll ask the Ranking Member to help me here.

And I'll start with you, Mr. Hoover. You mentioned IPAW. And I know it's the process of identifying the technical challenges to what we want to accomplish. What are some of those technical challenges that we're facing? And how can we address them?

Mr. HOOVER. Thank you for that, Mr. Chairman.

It's important to realize that, as we've tried to put this system in place, we've focused, really, on the method of distribution, and we haven't looked at what the message is and—because we want to make sure that we have those technological challenges, we understand what they are, so that as we transmit an emergency message to a cell phone provider, for example, they don't have to do anything to the message, and it can go right straight through their system. So, one of the technological challenges that we're working with—and I would say there are two of them—the first one is what I would call that middleware. There needs to be some type of a software application that will allow us to send a message to, for example, the cell phone carriers or the satellite radio providers, some software that will allow the message to go right from an authorized, authenticated originator of a message into their system without the provider having to manipulate the message and then go out to their service customers. So, that's the first challenge, is trying to develop that, sort of, middleware piece, and we have——

Senator DEMINT. Are you working with the private companies on doing—my concern is, I think, too often in government we'll develop our own ideas of what should be done, and then tell the carriers, "Here, use this."

Mr. HOOVER. Right.

Senator DEMINT. And they may have to spend incredible amounts of money to adapt to what we've developed. And it would seem a much better approach that if we find out from them how they need this information, so that they can pass it straight through—and you're telling me, that is——

Mr. HOOVER. We're doing that.

Senator DEMINT.—your approach.

Mr. HOOVER. And, actually, we are doing that, and we're doing that with all the participants in our digital pilot that we're doing here with the—in the national capital region, and we're getting ready to move out into phase two.

All of the folks that are at the table with us, through voluntary participation—the cell phone folks, the satellite radio folks, commercial broadcasters, all the different people involved, even the technological—the technology development folks—are involved with us, and we have put together a group to address those technological issues that really are going to make the system work.

Senator DEMINT. So, your perspective may be that the Federal agencies, working together, may actually create different methods of distribution in order to work with all of your customers, which, in effect, are the various carriers, cell phone, whatever, that——

Mr. HOOVER. Yes, sir.

Senator DEMINT.—you're going to try to adapt to them.

Mr. HOOVER. Yes, sir. And the key to it is that Common Alerting Protocol that we've adopted and we've been using in our pilot programs, so that the message is in a digital format. It's a packet of ones and zeros, basically. It doesn't matter what the message is. If

we can keep it in a Common Alerting Protocol format, any type of a receiver device that's in the digital age should be able to take that message and send it out.

Senator DEMINT. Just—and this question could be to any of you. Going through the process of setting this whole system up is, obviously, our responsibility. But a part of that is trying to understand how people will respond. And, in many cases, we may spend a lot of time and money doing something where people will not necessarily respond in a constructive way. But is that part of this consideration? And I know we've maybe observed, through weather alerts or whatever, how many people actually will do anything about it. Are we into the behavior of our final customer, here, the citizen, and how they might behave when they get an alert?

Mr. HOOVER. Sir, let me start with that, and then maybe Mark can finish up, because I know they've done a lot of work in the social-behavior piece.

As I mentioned, our focus has been on the technology, at the moment, and we haven't so much focused on the message. But that will be the next piece of it, as we move forward, is to figure out, OK, what are those messages that we want to send so that we do give people the right information that can save lives? And I know that NOAA has done a significant amount of research in social behavior in that area.

Mr. PAESE. Yes, thank you, Reynold.

Yes, as Reynold mentioned, we believe that setting the architecture and the protocols and the infrastructure, I think, are our first stage to get the architecture set up, and learning from the lessons that NOAA has and with the behavioral scientists that we've spoken to on—when a message goes out, what actions to take and what message to provide them. We're going to use that as a basis, then, to continue on.

Senator DEMINT. Senator Nelson?

Senator BEN NELSON. Thank you, Mr. Chairman.

Well, as you have seen, Chairman Stevens is quite subtle.

[Laughter.]

Senator BEN NELSON. I want to examine your approach to dealing with how you bring together architecture and differentiation of message in the ordinary course of things, where you have to start out with the ability to notify and then you have to decide what it is that you want to say and, of course, ultimately, the audience for the message. But this is probably very time sensitive because of the terrorist threats that are represented today.

Therefore, I think people will feel more secure if there's notification. They'd feel most secure if they don't think there's going to be a terrorist activity. On the other hand, I think people are wise enough to know that zero tolerance may be our goal, but it's hard to achieve. So, the second best is to have some degree of notification, because of what that would represent in their preparedness.

As you're doing this, with the technology, the hardware, and the software, are you going to be in a position, ultimately, to where the use of the technology would permit you to alert people, through the BlackBerry or through the cell phone, of a tornado in a certain area? Also, I assume that you're probably looking at area codes. There may be some other technology that you use that would iden-

tify it. Are you going to be able, at some point, to be that specific in your alerting system? As you choose.

Mr. HOOVER. Yes, Senator. In fact, one of the parts of the IPAWS is a partnership we're doing with NOAA for GTAS, the Geo-Targeted Alert and Warning System, where we'll actually be able to use the reverse-911 database to provide targeted warnings to precise groups of people, based on the 911 database and other systems that NOAA has in place, to give them warning, to say, "There's a tornado coming," and, "Head in a different direction," or some specific message and instruction. So, we are doing that. And I think in the next panel you'll see a demonstration where we're able to use an alert and warning message and generate it through a number of different devices, including the BlackBerry and other devices that are out there.

Senator BEN NELSON. Mr. Paese?

Mr. PAESE. Yes, if I may. Yes, we believe that is the wave of the future. Obviously, FIPS codes, the way we alert and warn people today by county and—it can be broken up into a ninth of a county. But GIS, we believe, is the future. If a person in a location can get a message, a signal, if you will, on their BlackBerry, on their cell phone, on their device, that, we believe, is the way to geo-target individuals. And the technology is there today. We feel that integrating that technology into the front end of the message to get it to those individuals is the key, and we feel that is the future.

Senator BEN NELSON. Well, as you proceed, I think the question is, how quickly can you achieve that, and what sort of timeline can you put in place so that your progress can be measured, not only by yourselves, but by others from the outside? I think that's the frustration you're sensing. When we don't know whether you're 50 percent toward your objective, or 35, or 5 percent toward it, it's difficult for us to provide the kind of oversight that we think we need to provide.

In that regard, because there's more to this, at times, than the technology and the differentiation, Mr. Moran, how do you expect the FCC to proceed in the rulemaking that is probably going to be necessary? Because we're talking about some of the basic nuts and bolts, as well as the technology and the program itself.

Mr. MORAN. Yes, Senator.

We have—last summer, we opened a proceeding on improving the alert and warning systems, and we got an extensive—we have an extensive written record from that proceeding. We asked a number of questions, many of them you've actually—you and the—Chairman DeMint have touched on. We've asked many of those questions in our proceeding. We got an—we have an extensive record, and we've been in—recently, we've been in touch—we've had a series of meetings with all the major media players to try to figure out how we can improve the EAS system and what additional augmentation to the processes, to the alert and warning systems, may be necessary.

So, we have quite an extensive record. We expect to be able to deliver, perhaps, an initial order that would make some initial improvements to the EAS system in the next several months.

Senator BEN NELSON. Could you narrow that down just a little bit?

Mr. MORAN. We expect to be able to bring something for Commission decision in the next several months on some basic issues of participation in the EAS program by digital broadcasters, by satellite, direct-to-home TV and radio broadcasters—or service providers.

Our approach is to set some basic goals and obligations that would—missions, goals that we would try to meet, and to allow some flexibility so that the cost to the providers would not be that much to implement what is desired.

So, we do intend to have some flexibility to make sure that the basic goal, that all American citizens would have access to an excellent emergency warning system—that's the goal. We would allow some flexibility, if that's what it takes to make it happen, with the infrastructure that's out there.

Senator BEN NELSON. A short question to follow up on that is, will the rulemaking proceed at an appropriate pace to make sure that we don't get to the end of the line with the technology all ready to go and we've got several months waiting for the rulemaking to be complete?

Mr. HOOVER. Maybe I can take that one, Senator. We—part and parcel with the FCC's rulemaking initiative, as NOAA had pointed out—Mark mentioned in his testimony—we co-chair a Task Force on Effective Warning that has all the major players in the Federal Government involved in alert and warning. Our objective there is to develop a national policy that will lay out the architecture for a national alert and warning system. And we hope that that policy will fit part and parcel with the FCC's rulemaking. And I think we're working to try to get that done, as a——

Senator BEN NELSON. So, we could——

Mr. HOOVER.—on a very timely basis.

Senator BEN NELSON.—we could reach closure on the actual system and the authority that is there, any authority that's required, and not be held up by even pending legislation that might become necessary.

Mr. HOOVER. That's correct. We're trying to marry up a national policy for alert and warning that we think will include—and we're pretty confident will include—this IPAWS solution that we're talking about today, and marry that up with the rulemaking so that the policy will help the rulemaking, as opposed to the rulemaking driving the policy or being hindered by anything else.

Senator BEN NELSON. Well, I think that's excellent. And it needs to work that way, or I don't think you'll want to attend the next hearing when the Chairman is here.

[Laughter.]

Senator BEN NELSON. Thank you very much.

Thank you, Mr. Chairman.

Mr. HOOVER. Thank you, sir.

Senator DEMINT. I'm, kind of, sitting here wondering why we're working on legislation if you're doing the policy and rulemaking here. So, you're initiating this without legislation. Is——

Mr. HOOVER. Yes, sir. One of the things that—we've started this about a year and a half, almost 2 years, ago.

Senator DEMINT. Yes.

Mr. HOOVER. And we started with this IPAWS solution, when APTS, Public Television folks, came to us and said, "We want to be a partner with Homeland Security in providing alert and warning messaging." At the same time, the FCC had their Media Security and Reliability Council that came and made recommendations on improvements to the EAS. At the same time that that hit, the Partnership for Public Warning produced a report that had a number of recommendations in there. We think we're implementing most of those recommendations. And we started moving down the road to developing this IPAWS solution, and what we realized is—between us and NOAA, that we need the policy that will show us what the architecture is, at the end of the day, because we can put all these things together—the technology is there; it's that integration piece. And so, the White House stood up this Task Force on Effective Warning, just in the last 2 or 3 months, and we're on a pretty fast track to try to deliver a policy so that it lays out what does that end state look like for a next-generation alert and warning system. And we're working very closely with the FCC so that all of those things happen together.

Senator DEMINT. So, if we don't develop legislative guidelines, you're going to do it anyway, right?

Mr. HOOVER. Yes, sir.

Senator DEMINT. OK. I guess that's a good challenge to have here.

[Laughter.]

Senator DEMINT. Mr. Moran, let me ask you a question, because I'm very concerned about us developing something that—issuing mandates to the private market that could cause considerable cost and maybe not necessarily take advantage of evolving technologies. You mentioned some flexibility. You know, my hope would be that—and I would like your opinion on this; maybe I should state it that way—is, if we make the messaging, the distribution available in a lot of different formats that can be accepted by a vast array of carriers, is there any reason that we cannot make the acceptance of this voluntary by the carriers?

Mr. MORAN. In our proceeding, we've actually asked the question—currently the delivery of the state and local message is voluntary under our current rules. We've asked the question whether it should remain voluntary——

Senator DEMINT. So, are you actually considering issuing a mandate that all—everyone would have to take whatever——

Mr. MORAN. Well, we've——

Senator DEMINT.—you send out?

Mr. MORAN.—asked the question, and we've got quite an extensive record on that. There are some parties who believe it should be mandatory, on the record, and there are others who believe that voluntary is fine. Some have argued that the voluntary aspect has worked very well over the years and it should be allowed to continue.

All I can tell you is, we have parties on both sides of that issue in this proceeding, and we are looking at that and studying that, and it would have to be brought to the Commission for a decision on that.

Senator DEMINT. Well, if my opinion matters, I happen to believe, at this point, that it's likely, if it's voluntary with full disclosure—in other words, if I get a cell phone and it has disclosure that it does not include the warning, that our carriers would very quickly create a competitive advantage for themselves by doing it better and better, and we would have a best-practices system that could allow the system to evolve and improve, other than stick to a standard that we create here this time. But that's just my opinion at this point.

And one other—just a quick question. I assume hard-line phones are being considered as part of this, as a message, because—since a lot of people are at work. Right? They're in——

Mr. HOOVER. Yes, sir. And that's part of that whole—the GTAS, the Geo–Targeted Alert and Warning, can use the land-line phone system.

Senator DEMINT. Senator Nelson, any additional questions?

Senator BEN NELSON. Would the differentiation of warnings and message and the audience that would receive the warnings—in narrowing that down, what would you encounter, in terms of difficulties, or will that be coming forth in the second panel, where they do a demonstration? Will there be some sort of regulatory problem? Is there a privacy issue here? What would be involved?

Mr. HOOVER. I guess I'm not quite clear on what the question is.

Senator BEN NELSON. Well, would I have to sign and say that I want to be notified, or will it be an automatic benefit or service included within the technology that I happen to have?

Mr. HOOVER. I think one of the pieces of the IPAWS that we're doing, and I mentioned in my remarks, is that we're looking at an AMBER-Alert-like portal, and we're trying to build on the success that the Department of Justice has had in disseminating alert and warning messages using their AMBER Alert system, so that in the—at the present time, what we're considering is an opt-in situation, so that you would go to a website that would allow you to opt into the types of messages that you would like—alert and warning messages you would like to receive, and that the only real mandatory message, at this point, as we move down the road, would be the carriage of a Presidential-level national emergency message that you're going to get regardless of if you sign up for it or not. We just believe that if you require every message to be carried, it's going to go the way of the car alarm and people aren't going to pay attention to the ones that really are important to them, but folks will go online—and you can go on to this website, to the portal, and say, "I want to be notified of earthquakes and tsunamis and tornadoes," whatever those things might be, terrorist attack, and you would get those appropriate messages.

Senator BEN NELSON. If you get this perfected—and I hope that you do—will you promise me that you'll take over the warning system as to when we need to evacuate the Capitol?

[Laughter.]

Senator BEN NELSON. Get that at some level that we can appreciate it?

Senator DEMINT. Yes, let's just hope we don't have to evacuate, this week, right?

Senator BEN NELSON. That's right. Will there be an extra cost to the consumer for the messages? Will I have to pay for my equipment?

Mr. HOOVER. You know, Senator, I can't answer that question. Perhaps the private-sector folks in the next panel may be able to better address the costs that may be involved.

Senator BEN NELSON. OK.

Thank you, Mr. Chairman. Thank you all.

Senator DEMINT. It's been very productive. I appreciate it.

Let's switch out panels. We go from the first to the second. I thank all of you, gentlemen.

[Pause.]

Senator DEMINT. Thank you folks for being here. This second panel is composed of Mr. Richard Taylor. He's Chair of COMCARE Alliance. Mr. Taylor will be providing a perspective of the emergency-management community on what tools they need in a public-alert system.

Joining him is Mr. Christopher E. Guttman-McCabe, Assistant Vice President of Regulatory Policy and Homeland Security at CTIA.

Senator DEMINT. Mr. Guttman-McCabe will be discussing the cellular industry's participation in recent emergency-alert projects and discuss the industry's perspective on their participation in the next-generation emergency-alert system.

And finally appearing is Mr. John Lawson, of the Association of Public Television Stations. I understand Mr. Lawson is going to run through a demonstration of the digital emergency alert system.

I'll ask Mr. Lawson to begin the demonstration and provide a short summary of his testimony.

So, Mr. Lawson, if you can begin?

## STATEMENT OF JOHN M. LAWSON, PRESIDENT/CEO, ASSOCIATION OF PUBLIC TELEVISION STATIONS

Mr. LAWSON. Good morning, Mr. Chairman, Ranking Member Nelson. Thanks for inviting me to testify today on behalf of our members, which are the local public stations across the country. I'm here to address the development of an all-hazards multiple-devices warning system and the dual-use contribution that public digital television can make.

Digital television, DTV, is really a very powerful wireless data distribution platform, in addition to HDTV and/or multiple programming streams, where we now have just one. DTV also can send very high-end data to a number of devices. When we broadcast data, also called datacasting, information is embedded in the over-the-air digital signal. This data can be received on PCs and laptops equipped with commercial off-the-shelf DTV tuner cards. This little silver box on the front of this table here is an example of that. This means very low-cost access for first-responders, as well as schools, hospitals, and other institutions. Datacasting uses only a fraction of the digital spectrum, and it can run simultaneously with HDTV or whatever the station that's broadcasting to viewers. If needed, the data can be encrypted so that only certain computers—for example, in police departments—can access it.

Datacasting is completely scalable and is bottleneck-free. Just as with broadcasting to TV sets, the information can be received by one viewer or one million viewers without fear of overload. Typical DTV signals can reach 50 to 60 miles from a single transmitter.

As you heard from Reynold Hoover, APTS, last fall, entered into a cooperative agreement with FEMA at DHS to launch a pilot project in the national capital region. This pilot is serving as the basis for the new Digital Emergency Alert System, or DEAS. APTS is joined by PBS and public stations WETA, here, Maryland Public Television, the New Jersey Network, WHRO, in Norfolk, and KAKM, in Anchorage, as well as commercial media and wireless partners.

Our pilot is demonstrated graphically on the flowchart at the side of the room, and I'd be glad to take you through that during Q&A.

We're now going to demonstrate for you the capabilities of our DEAS pilot. At this moment, an official at FEMA is sending a test alert to the PBS Satellite Operations Center in Springfield. PBS is uplinking the alert, and it's being received by WETA. Instantaneously, without anyone at the station touching it, WETA DTV retransmits the alert over the air within its digital signal. DHS has the ability to provide text, as well as audio and video. In this case, we're transmitting all three.

We can also—once a Presidential message from FEMA comes through, however, it takes priority. All of this comes over the air to a computer here via the small antenna on the table in front of the panel. This is off-air. This small v-shaped antenna here, a Radio Shack antenna, is actually receiving the WETA signal off-air. It's connected to a laptop computer over there, which is projecting the alert on the screen.

So, we can send video, as is opening up right now, which shows you the flexibility of this system. We can send the text messages. We can send the audio alerts. This is live from FEMA.

This is coming over XM satellite radio. And the cell phones are ringing, because, embedded in the alert, is data that goes to the headends of the cell phone companies, and they can retransmit that as a text message.

So, as Reynold described this morning, we are feeding these alerts to other radio and TV stations. We're feeding it to cable headends and cell phone and pager services. The cell phones are ringing because of the alert.

Along with the alerts, we can datacast text and animation files over WETA. One of those files is something you all, in the Senate, are quite familiar with, a quick-card evacuation information sheet. You can see on the screen, the file has just opened. This was sent as a file over the air, again, to PCs. A map you're familiar with is also being displayed. This information also can be sent through wireless through your BlackBerrys, all in a matter of seconds.

Datacasting can send just about any type of file. In the next example, we developed a simple animation, based on a dirty bomb going off at Metro Center. It forecasts the movement of the radioactive plume and indicates the traffic patterns that should be followed as part of the evacuation plan.

We can also datacast full motion video and audio of the President addressing the Nation, if necessary, or a mayor addressing a city.

The best practices developed during the DEAS pilot also are serving as a model for local jurisdictions. Stations around the country are entering partnerships with public safety and other agencies from areas around nuclear power, chemical plants, and the Las Vegas casinos. Alert systems are being tested. Stations also provide training, such as the port-security video we're seeing again.

As we work with FEMA to plan the national rollout of the DEAS, our members, the local public television stations, stand ready to play an integral part at the national, regional, state, and local levels.

I'm happy to answer any questions you may have.

[The prepared statement of Mr. Lawson follows:]

PREPARED STATEMENT OF JOHN M. LAWSON, PRESIDENT/CEO, ASSOCIATION OF PUBLIC TELEVISION STATIONS

Mr. Chairman, Ranking Member Nelson and Members of the Subcommittee:

It is my privilege to come before you today to discuss how Public Television's digital infrastructure can play a role—a dual-use role—in developing a new, robust and efficient digital emergency alert and warning system. No doubt this month's bombings in London continue to reverberate in the minds of the Members of this Subcommittee. To me, it is also a vivid reminder that our Nation's current Emergency Alert System is built on an aging analog infrastructure and must be upgraded.

But I am here to bring you good news. That state of affairs is beginning to change, and I'm pleased to report that Public Television, working directly with the Department of Homeland Security, is playing an integral role in the development of an all-devices, all-hazards, digitally-based emergency alert and warning system.

**Digital Emergency Alert System: DEAS**

The next generation of a national emergency alert system is called the Digital Emergency Alert System, or DEAS. It will be based on Public Television's digital transmission infrastructure. Like the current system, the DEAS is designed to ensure that the head of our national government—the President or his successor—can quickly communicate to the American public during an emergency. The current system—which, by the way, was never utilized during 9/11—is limited to two basic reception devices: radios and televisions. And yet today, Americans have become fluent in an impressive array of other—often, more portable—devices, including cell phones, personal computers, Blackberries and other PDAs. Under the DEAS, the President could potentially reach almost all Americans quickly with an important message delivered to any one or all of these devices.

It is also important to note that the current Emergency Alert System was conceived during the cold war era to provide warning for threats that were national in scope—namely, a nuclear attack. Today's most potent threat, acts of terrorism, are by their nature more local or regional in scope, as the residents of New York, Washington, Madrid and London can attest. That is why the new DEAS will provide a backbone that can be interconnected to deliver alert and warning at the local, regional and national levels.

**Role for Public Television**

Public Television is a mission-driven institution. When our system was faced with the prospect of undertaking a daunting conversion from an analog to digital transmission platform, we naturally began to explore the many ways that this exciting new digital technology could be used to benefit the American people. With the emergence of a digital broadcasting application called datacasting, which I will discuss further, we quickly grasped that local digital public television stations could play a role in enhancing public safety. At first the idea focused on natural disasters such as tornadoes. And then came 9/11.

The other critical feature of the Public Television system is our penetration: we reach nearly 99 percent of American households with analog service and, soon, with digital. Indeed, our system's breadth is impressive, but so is our depth. We are deeply rooted in our communities, typically among the most trusted local institutions and ones that have forged strong linkages to other community institutions and populations.

In short, Public Television is building out a fully integrated digital infrastructure which, once complete, will reach nearly every American community. The DEAS is a very cost-effective, dual-use application that builds on this infrastructure.

**What is Datacasting?**

In order to appreciate the capabilities of a DEAS, it is necessary to understand the central application involved—namely, datacasting. Digital television, or DTV, is most closely associated with high-definition television (HDTV). But DTV is really a powerful, wireless data transmission system. It is also very flexible. From a single transmitter, a broadcaster can send any mix of HDTV, multiple standard-definition channels, or high-end data to any DTV reception device within 50–60 miles.

One of these applications, called datacasting, is a one-way broadcast transmission of Internet Protocol (IP) information. The data being transmitted can take the form of text, video, audio, and graphics. Datacasting uses only a portion of the broadcast spectrum. Moreover, datacasting can deliver large amounts of data embedded in the broadcast signal at a rate of up to 19.4 megabits per second (MBPS)—the equivalent of up to 13 T–1 lines.

Datacasts are encoded within the digital television signal and then decoded by an inexpensive receiver that is easily hooked up to a personal computer, laptop or computer network. Reception can be achieved through a small portable antenna that sits on top of the PC (or laptop in the field), or users can receive the signal through a conventional rooftop TV antenna or cable. The signal can also be instantly retransmitted over wireless and other networks.

**Advantages of Datacasting**

Datacasting boasts several key attributes:

- *Datacasting is highly scalable and congestion-free.* It avoids the communications bottlenecks we saw in New York and Washington on 9/11. Because it is a broadcast medium, it takes no more bandwidth to reach millions of end-users simultaneously than it does a single end-user.
- *Datacasting is secure.* Through additional technology, data can be encrypted, rendering it far less vulnerable to hackers than Internet-based communication.
- *Datacasting is flexible.* It can be "addressed" through conditional access to a select group of end-users (such as a Federal agency, a local fire department or a school district) or made available to the widest possible audience—anyone with a digital antenna and receiver.

Included at the end of this testimony are several examples of current and ongoing Public Television datacasting projects, ranging from educational partnerships to robust public safety and training efforts. I highly recommend that the Subcommittee review these examples in order to appreciate the wide range of services being offered and explored by Public Television stations and their local and regional partners.

**Department of Homeland Security-APTS Pilot Program**

At this time, however, I would like to focus the Subcommittee's attention on one particularly important project that is being pursued jointly between the Department of Homeland Security and APTS.

In October, 2004, the Department of Homeland Security's Federal Emergency Management Agency (FEMA) signed a cooperative agreement with APTS to conduct a Digital Emergency Alert System—National Capital Region Pilot Project (DEAS–NCR). The pilot was launched to demonstrate how public television's digital infrastructure could be used to support the distribution of Presidential messages to the public and of digital all-hazards Emergency Alert System (EAS) messages to TVs, radios, personal computers, telephones and wireless networks.

Public broadcasting participants in the pilot include APTS, the Public Broadcasting Service (PBS), WETA–TV and FM, Maryland Public Television, WHRO (Norfolk, VA), KAKM (Anchorage, AK) and the New Jersey Network. These Public Television entities were joined by WTOP–AM radio, WRC–TV (both in Washington, D.C.), Comcast Cable, the National Cable & Telecommunications Association (NCTA) and XM Satellite Radio. Participating telecommunications industry organizations include Cingular Wireless, Nextel, T-Mobile, the Cellular Telecommunications and Internet Association (CTIA) and USA Mobility, among others.

Phase I of this pilot project focused primarily on testing whether emergency alert and warning messages could be successfully transmitted to end-users in a workable format—known as the Common Alerting Protocol (CAP) format. The Pilot was formulated around the concept of real-time activation by FEMA of simulated emer-

gency alert and warning messages into the DTV network of PBS and WETA, who redistribute the alert messaging to other participants in the pilot.

I am pleased to say that Phase I of the pilot project was a resounding success. We were able to demonstrate that this infrastructure works and works well.

**Phase II of the DEAS–NCR Pilot**

Based on the success of the first phase of the DEAS–NCR Pilot, the Department of Homeland Security has extended the pilot by an additional 6 months. The extended pilot program will lay the foundation for the national roll-out of a digitally-based Federal public safety alert and warning system.

Phase II has three major components.

- First, the Pilot will spend additional time on testing and evaluation, as well as provide an opportunity to further develop the components of the pilot system. Additional testing sites beyond those in Phase I of the pilot, including one or more state emergency operations centers (EOCs) and several additional public broadcast stations outside the National Capitol Region, are being incorporated in Phase II.
- Second, APTS will work in coordination with other alert and warning pilots and vendors, such as the one that DHS is developing to provide satellite connectivity to the Nation's current Primary Entry Point (PEP) stations. These other pilots are also consistent with DHS's goals for an Integrated Public Alert and Warning System (IPAWS) framework. The goal here is to ensure that a DEAS can work with, and be complementary to, other aspects of an improved national alert and warning system.
- Third is the development of a DEAS National Deployment Plan as well as a final DEAS Pilot Report for Congress. The DEAS National Deployment Plan will include construction and timeline estimates, technical risk determinations and other technical implementation options.

**Next Steps**

We at APTS are gratified to play a role in this effort, and our member stations are fully committed as well. We could not be more pleased with the way the DEAS–NCR Pilot has progressed and how that might translate to a fully developed, robust national alert and warning system. I would also like to commend Reynold Hoover and his colleagues at FEMA for their foresight in recognizing the dual-use features of DTV, and for forging a very productive working relationship with us.

Going forward, there are two elements that I have not yet mentioned that I believe are critical to the ultimate viability of the DEAS.

**Satellite Interconnection**

First is the replacement of Public Television's satellite interconnection system. As you are probably aware, national programming is currently distributed from PBS to the more than 350 local public television stations via a satellite interconnection system. That system is wearing out and is scheduled to go dark in October 2006—when the current leases on satellite transponders expire. Congress has funded two of four installments for a replacement, Next Generation Interconnection System over the past two appropriations cycles. Continued appropriations in FY 2006 are extremely important to secure long-term leases on new satellite capacity as well as enhanced terrestrial distribution capabilities. This is relevant to the subject of today's hearing, because the same infrastructure that ensures distribution of national programming also forms the backbone for distribution of emergency alert and warning messages under DEAS.

**Local Origination**

At the local level, it is also important that we plan for and provide resources for local origination equipment. The purpose of local origination is to allow local communities to take advantage of the Federal DEAS whenever emergencies of a local or regional nature occur. If, for example, a tsunami were to develop in the northern Pacific Ocean, headed toward Alaska and the Pacific Northwest, it would be essential that local stations have the ability to augment and enhance the level of communication about the tsunami to the affected citizenry.

Similarly, any number of communities that lie within the range of hurricanes—from Gulf States to the Atlantic seaboard—would benefit from a fully integrated local and national warning system that would enhance the NOAA weather service. Datacasting can be used not only to provide initial warning but also to distribute detailed information such as evacuation routes, instructions for sheltering in place and other safety tips. Information is crucial in any crisis, whether a chemical spill

at an industrial site, an incident at a nuclear power plant, or other man-made or natural disasters.

The ability to create and distribute local and regional messages and data packets is vital to a fully integrated emergency alert and warning system. It is in the best interest of the American people, who expect local and national coordination in times of crisis. Fortunately, the capability necessary to accomplish this is within our grasp.

**Conclusion**

Public Television is gratified that we can play a role in helping to shape our Nation's next generation emergency alert and warning system, and most importantly to deliver that capability. It is a natural extension of our public service mission. We believe that one day in the near future Public *Digital* Television will play a crucial role during a crisis that will save lives and calm fears.

Thank you for giving me the opportunity to testify today.

Senator DEMINT. Just a quick question and I want to get to the other panelists. As far as our BlackBerrys are concerned, would our server have to coordinate with you for it to come through my BlackBerry, or could that just be automatic?

Mr. LAWSON. By arrangement with the service provider—and I don't know who you use, in the Senate—it would be passed through automatically.

Senator DEMINT. OK.

Mr. LAWSON. Your server would not—as I understand it; and I don't understand the Senate firewalls—but, generally speaking, no one's touching this data. If, by prior arrangement, your service provider has agreed to handle this messaging, no one touches it; it goes right through.

Senator DEMINT. So, the servers of these BlackBerrys, regardless of the Senate or what—does not—they don't necessarily have to have a lot of new technology, or whatever, to do it?

Mr. LAWSON. This is why—the Common Alerting Protocol and the Integrated—the IPAWS that the witnesses testified about this morning, make sure that it passes through. There is nothing extra on the receive end, in terms of the text messaging, that would be necessary.

Senator DEMINT. I'll save my other questions. But, since I've spoken, Senator Nelson, if you wanted to say anything——

Senator BEN NELSON. Now, for example, a cell phone was ringing. Is that technology aimed at some sort of GPS or by area code? What if I have an area code from Nebraska on my cell phone, but I'm located here? Does it contact me? What may be important here, in terms of a localized disaster, might not be important out there, vice versa.

Mr. LAWSON. I know that FEMA and NOAA are working on the geographical targeting. Our pilot doesn't do that. But I can tell you that it does—this system fully supports conditional access. The signal goes out to everyone, but only certain devices, such as Senate BlackBerrys, might have the authorization to receive it. It might be card, it might a code, it might be a thumbprint. So, we can segment that way. Also, although we're sending information, this test data, over the PBS satellite, so anything public state or state network, like Nebraska ETV in the Nation, can take it. You automatically have geographic localization of that kind, at least on the state and national—regional level.

Senator BEN NELSON. OK, thank you.

Senator DEMINT. Mr. Guttman-McCabe?

**STATEMENT OF CHRISTOPHER GUTTMAN-MCCABE, ASSISTANT VICE PRESIDENT, HOMELAND SECURITY AND REGULATORY POLICY, CTIA—THE WIRELESS ASSOCIATION™**

Mr. GUTTMAN-MCCABE. Thank you.

Good morning, Chairman DeMint and Senator Nelson. I am Christopher Guttman-McCabe, Assistant Vice President for Homeland Security and Regulatory Policy at CTIA—The Wireless Association.™

I am privileged to appear before you today to discuss the wireless industry's efforts regarding an all-hazards network.

The wireless industry recognizes the importance of this effort. CTIA and the industry have dedicated significant resources to address this issue. We have coordinated our efforts through the Department of Homeland Security and FEMA. The industry also recently launched a wireless AMBER Alert project that not only will help to protect our Nation's children, but also will provide a useful template as the industry moves forward with an emergency alert service.

The wireless industry, like many other high-tech industries, is in a process of continual change and renewal. The industry has invested billions of dollars in its networks, and consumers have invested billions of dollars in their handsets, their wireless PDAs, and their data cards. Manufacturers and service providers unveil new capabilities almost daily. New technologies and services are likely to extend both the reach and the capacity of wireless. A sensible emergency alerting policy must take into account both the massive investment in place today and investment that defines the capabilities that can be used this year, as well as next, and the technological developments that propel the industry in the long run.

CTIA, working with the industry, has initiated a two-part approach to the emergency alert issue. The goal is to balance the industry's existing capabilities with the perceived requirements of emergency alert service, at the same time recognizing that the industry is evolving. Unlike the existing emergency alert service which operates on a broadcast network designed to transmit messages from one point to multiple points, the existing wireless was designed to be point-to-point, one customer to another customer.

Accordingly, the industry is partnering with FEMA on a pilot project, that you heard Mr. Hoover talk about earlier, that will initially utilize the industry's text-message capability, its SMS capabilities. While there are both limitations on the number of SMS messages that can be sent during any one period of time, as well as on the number of characters that can be contained in any one single message, there is one significant benefit to the short-term use of SMS, and that is that it is available today. However, this initial service must be approached with caution, as the limitations and concerns regarding both capacity and message content are likely to arise during an emergency.

As part of the second, longer-term element of the industry's effort, CTIA and the industry are investigating mechanisms for geographic delivery of messages. This second-stage effort is designed

to take advantage of the constant evolution that is a hallmark of our industry. The industry is looking into what role, if any, capabilities such as cell broadcasts could play in the emergency alert environment. Additionally, the industry is investigating other potential delivery mechanisms, including whether the existing NOAA service could be incorporated into a wireless phone, as well as whether SMS messages can be targeted geographically.

Several of the capabilities being investigated for longer-term delivery would require the industry to address issues including standardization, product development and deployment, and, possibly, handset replacement. In the interim, CTIA continues to work with FEMA on the creation of a framework for development of an alert service that ultimately can be transmitted on multiple retransmission media. CTIA and the industry believe that any emergency alert service should not focus solely on the wireless network, as the networks are not currently designed to pass messages to all active subscribers simultaneously. Rather, an emergency alert service should utilize the full range of communications devices, such as phones, e-mail, and instant messaging, radios, television sets, and satellite.

The efforts discussed above are only part of the work being done in this area. More work needs to be completed, and, ultimately, government can help. A true government-industry partnership, as occurred during the creation of the wireless priority service, will aid in that development. CTIA and the industry believe that it is counterproductive to have a statutory mandate in this environment. Application of the wireless priority service model of government-industry partnership will lead to a solution that takes advantage of the industry's creativity and ingenuity.

As government and industry move forward with both a short-term and possibly longer-term solution, addressing issues including liability relief, establishment of a service description, designation of an authority for development, as well as operation of the alert service, and funding, will be beneficial. CTIA and the industry look forward to continuing the partnership between government and industry.

Thank you, again, for this opportunity to discuss the wireless industry's efforts. We look forward to working with you and your staffs toward a service that will benefit American. And I look forward to addressing any questions that you might have.

Thank you.

[The prepared statement of Mr. Guttman-McCabe follows:]

PREPARED STATEMENT OF CHRISTOPHER GUTTMAN-MCCABE, ASSISTANT VICE PRESIDENT, HOMELAND SECURITY AND REGULATORY POLICY, CTIA—THE WIRELESS ASSOCIATION™

Good morning Chairman DeMint, Ranking Member Nelson, and distinguished members of the Subcommittee. I am Christopher Guttman-McCabe, Assistant Vice President for Homeland Security and Regulatory Policy at CTIA, The Wireless Association.™ CTIA is the international organization that represents all sectors of the wireless communications industry: wireless carriers, manufacturers, and data companies. I am privileged to appear before you today to discuss the wireless industry's efforts regarding creation of an all hazards network and what role government can play in that effort.

The wireless industry recognizes the importance of this effort. CTIA and the industry have dedicated resources to examine this issue and are working toward an

emergency alert capability. CTIA and the industry have coordinated their efforts with the Department of Homeland Security and the Federal Emergency Management Agency (FEMA), as well as with the Federal Communications Commission. As discussed below, the industry also recently launched a voluntary Wireless AMBER Alert Service that not only will help to protect our Nation's children, but also may provide a useful template as the industry moves forward with an Emergency Alert service. While the AMBER alert service differs from an Emergency Alert service in that the AMBER Alerts are not necessarily initiated during a time of severe network congestions (as is likely the case in the context of an Emergency Alert), the industry already has begun to learn from the provision of this service.

**Background**

The wireless industry, like many other high-tech industries, is in a process of continual change and renewal. The wireless industry has invested billions of dollars in their networks. Additionally, consumers also have invested billions in handsets, wireless PDAs, and data cards. The industry runs on a mix of technologies varying from first generation analog to the latest third-generation designs. Manufacturers and service providers unveil new capabilities every few days. New technologies and services are likely to extend both the reach and capacity of wireless. Unfortunately, we do not know today what all those new capabilities will be or when they will become available. A sensible emergency alerting policy must take into account both the massive investment in place today—an investment that defines the capabilities that can be used this year and next—and the technological developments that propel the industry in the long run.

Developing a national emergency alerting policy should not be a one-time event. Going forward, there should be a continuing process for identifying the emergency alert environment, as well as industry capabilities. Uses and expectations of the service will indicate what may be appropriate for capacity of message delivery in the short term and long term. Further, the scope of who uses the system and for what purpose is very important to understand as it relates to the cost to develop, the management of the service, and effectiveness of the system.

CTIA, working with the industry, has initiated a two-part approach toward development of an Emergency Alert capability. The goal is to balance the industry's existing capabilities with the perceived requirements of an Emergency Alert service, at the same time recognizing that the industry is evolving. The continued evolution of the industry likely will result in different options being considered for delivery of Emergency Alert messages. For example, currently there is nothing deployed in the network for delivering messages to a specific targeted geographic area. Handsets and/or networks would have to be upgraded or replaced in order to provide such a service, and development and deployment of any geographic service would take time.

Accordingly, CTIA and the industry are initially working within existing capabilities to establish and initiate a voluntary effort to deliver Presidential-level Emergency Alert messages via Short Message Service (SMS), or text message, to those subscribers that opt in to a participating carrier. As discussed below, CTIA and the wireless industry are partnering with FEMA on a pilot project that initially will utilize the industry's existing SMS, or text message, capabilities. The SMS capability exists in the majority of handsets, and is provided by the overwhelming majority of carriers.

While there are both limitations on the number of SMS messages that can be sent during any one period of time, as well as limitations on the number of characters that can be contained in any single message, there is one significant benefit to the short-term use of SMS—it is available today. Utilizing SMS initially will work to avoid a significant amount of the development time frame that will accompany the solutions discussed below. However, this initial service must be approached with caution, as the limitations and concerns regarding both capacity and message content are likely to arise during an emergency.

Unlike the existing Emergency Alert network, which operates on broadcast networks designed to transmit messages from one point to multiple points, the existing wireless network was designed to be point to point—one customer to another customer, where the network has to route calls and text messages using switches and databases to direct traffic to individual users. In this environment, utilization of SMS to retransmit messages likely will result in latency of delivery of the message to consumers. However, as was concluded in the Wireless AMBER Alert context, an SMS offering—despite its expected limitations—is the best existing, short-term option for delivery of alert messages.

Second, as part of the longer term effort going forward, CTIA and the industry are investigating mechanisms for geographic delivery of messages. This second stage

effort is designed to take advantage of the constant evolution that is the hallmark of the wireless industry. The goal is to address the capacity issues that are part of any SMS-based alert service, as well as to develop a capability for targeting messages geographically. The capability to deliver messages geographically currently does not exist in wireless networks in the United States. Wireless service is based on point-to-point communications, and has not been designed for point-to-multipoint broadcast.

The industry is looking into what role, if any, services such as cell broadcast could ultimately play in the Emergency Alert environment. Additionally, the industry is investigating whether the existing National Oceanic and Atmospheric Administration (NOAA) service can be incorporated into a wireless phone, as well as whether SMS messages can be targeted geographically. Recent developments, including but not limited to broadcast offerings on wireless phones, as well as services such as Qualcomm's proposed MediaFlo offering, highlight how the industry and its technology are in transition.

Several of the capabilities being investigated for a geographic-based service would require the industry to address issues including standardization (both of the underlying product as well as the alert development and delivery process), product development and deployment, as well as the need for handset turnover if the service is not available in existing handsets. In the interim, CTIA continues to work with FEMA on the creation of a framework for development of an alert service that ultimately can be transmitted on multiple retransmission media, including wireless. CTIA and the industry believe, however, that while wireless can be a component of any alerting service, any Emergency Alert service should not focus solely on the wireless network, as the wireless networks are not currently designed to pass a message to all active subscribers simultaneously. Rather, an Emergency Alert service should utilize the full range of communications devices, such as wireline and wireless telephones, e-mail and instant messaging systems, radios and television sets.

**FEMA Capitol Region Pilot Project**

CTIA has been working diligently with carriers, manufacturers, and FEMA on a digital Emergency Alert pilot project in the national capitol region. The pilot project, being directed by FEMA, coordinated with the Association of Public Television Stations (APTS), and utilizing the digital broadcast spectrum, is designed to provide the Nation with an enhanced alert system. The goal of the first phase of the project was a "proof of concept" that Emergency Alert messages can be sent from FEMA to public broadcasters, imbedded in the digital broadcast spectrum, and then re-transmitted to third parties, including wireless carriers. A portion of the imbedded Emergency Alert message contained a text file that the wireless carriers were able to extract. Phase 1 of the pilot project has successfully been completed.

As part of the second phase of the pilot project, FEMA, APTS, and the five nationwide wireless carriers that are participating in the project will now focus on making the service scaleable so that messages that are initiated by FEMA ultimately can be passed through directly to the wireless carriers' networks. To date, several of the carriers have successfully re-transmitted a test message to a small portion of their employee base. The goal is to ensure that a system is in place whereby a message can originate at FEMA, and be transmitted and retransmitted without ever being edited, touched, or handled by any of the participating companies. Ultimately, Phase II of the pilot project envisions that an Emergency Alert message will be retransmitted to some portion of the carriers' customer base.

As discussed above, the carriers, initially, will utilize their existing SMS capabilities to retransmit a text message to customers that opt-in to receive the alerts. Ultimately, carriers may use one of the other longer-term methods being considered to retransmit the message to a specific geographic location. Whatever method a company chooses to utilize for retransmission, the industry is looking forward to completion of an Emergency Alert *process* that ultimately can take advantage of any of the new capabilities or services that will emerge from this highly innovative industry.

**AMBER Alerts**

The industry already is pursuing use of the wireless phone for the safety of the country. On its own initiative, the industry has launched a Wireless AMBER Alert Service that will provide another level of safety to its customers and the American public. This service enhances the industry's vast array of socially responsible initiatives. Partnering with the National Center for Missing & Exploited Children (NCMEC) as well as the Department of Justice (the designated national AMBER Alert coordinator), the wireless industry is making potentially life-saving AMBER Alert text messages available to wireless subscribers who "opt-in" to the offering.

The carriers currently participating collectively provide service to more than 90 percent of U.S. wireless customers. The service has been designed to be scaleable so that additional carriers can continue to join the effort going forward.

Wireless AMBER Alerts will significantly increase the reach of the AMBER Alert notification program. Past experiences indicate the first 3 hours are critical to the successful recovery of an abducted child, and the Wireless AMBER Alerts will be an invaluable tool in assisting the search process. According to the NCMEC, Wireless AMBER Alerts will potentially serve as a preventive tool as well. People who prey on innocent children will perhaps think twice before carrying out their malicious acts, knowing that almost any cell phone owner they pass could identify a perpetrator and have access to the immediate means to guide law enforcement officials to their location.

Under the program, the subscribers of participating carriers may "opt-in" to receive Wireless AMBER Alerts, and may do so at *www.wirelessAMBERalerts.org,* or by visiting their wireless service provider's website.

**Going Forward**

The efforts discussed above are only a part of the work being done in this area. More work needs to be completed, and, ultimately, government can help. A true government/industry partnership will facilitate development and deployment of the service. The wireless industry has in its immediate past an example of what can happen when government and industry partner voluntarily on the creation of a new service—Wireless Priority Service. Wireless Priority Service is a White House-directed National Security/Emergency Preparedness program, through the National Communications System, that utilizes the commercial wireless networks to deliver priority access to key government officials during times of crisis and high call volume. Government, through both the National Communications System and the Federal Communications Commission, worked with industry on development of the requirements for the service, but did not mandate a solution. Instead, government has provided funding to manufacturers and vendors for development of the capability, resulting in rapid deployment of the service in two phases.

CTIA and the wireless industry believe that it is counter-productive to have a statutory mandate in this environment. Application of the Wireless Priority Service model of government/industry partnership will lead to a solution that takes advantage of the industry's creativity and ingenuity. As government and industry move forward with both a short-term and possibly longer-term solution, the following are some of the issues that would benefit from joint government/industry consideration:

- *Liability relief.* As with the Broadcasters that currently provide the Emergency Alert service, the industry requires full liability protection for delivery of any Emergency Alert message, both for any short-term solution and any longer-term solution.
- *Service Description.* A joint government/industry partnership to develop the requirements of any emergency alert service that ultimately would result in the development and adoption of standards. This partnership will allow manufacturers to build to specific requirements.
- *Designation of Authority for Development of an Emergency Alert Service.* Designation of a specific authority responsible for balancing local, state and Federal requirements against industry capabilities.
- *Designation of Authority for Operation of an Emergency Alert Service.* Designation of a specific authority tasked with operation of the Emergency Alert service as well as creation of a clear set of rules governing who is permitted to generate messages and under what circumstances they can be generated, coupled with a process to authenticate and secure any Emergency Alert messages. Due to the possibility of a hoax transmission, this process must guarantee the integrity of the messages from the point of origination to delivery.
- *Research, Development, Deployment and Implementation Support.* The provision of funding to support research and development, as well as deployment and implementation, will benefit the establishment of a nationwide alert service.

**Conclusion**

CTIA and the industry look forward to continuing the partnership between government and industry toward development of an Emergency Alert service. Thank you again for this opportunity to discuss the wireless industry's efforts that could contribute to an all hazards network and what role the Government should play in that effort. We look forward to working with you and your staff toward a service that will benefit America.

Senator DEMINT. Thank you.
Mr. Taylor?

**STATEMENT OF RICHARD TAYLOR, EXECUTIVE DIRECTOR, NORTH CAROLINA WIRELESS 911 BOARD; CHAIRMAN, THE COMCARE ALLIANCE AND E–911 INSTITUTE; PARTNER, THE NATIONAL EMERGENCY ALERTING AND RESPONSE SYSTEMS INITIATIVE (NEARS)**

Mr. TAYLOR. Good morning, Mr. Chairman and Senator Nelson. Thank you so much for the opportunity to testify.

My name is Richard Taylor. I'm the Executive Director of the North Carolina Wireless 911 Board. I also have the privilege of chairing the COMCARE Alliance. I am also Chair of the E–911 Institute. And today there are few issues that are more important to our members than the one that we're discussing here and now.

COMCARE is a national nonprofit alliance dedicated to advancing emergency response. COMCARE is unique in that we represent the wide diversity of the emergency-response community.

I am also testifying on behalf of the National Emergency Alerting and Response Systems Initiative, or NEARS. The 17 national organizations that are NEARS partners represent over 40,000 individual agencies and over 400,000 individuals in the emergency-response profession.

The most effective public warning system is one that achieves the greatest possible reach. It is one that is used for all-hazards reporting, not just for specific incidents. However, there will never be one system that solves the problem. An interoperable solution for public warning will not be achieved by purchasing a new national emergency-alert network for the 100,000-plus emergency agencies, much less solve the other public and private organizations that need to be part of an emergency network.

We must focus on connecting these emergency agencies through one system of systems, or an internetwork. This emergency internetwork will allow these organizations to contact the public through growing numbers of consumer devices.

Another key component is emergency data standards for public warning. The Common Alerting Protocol fundamentally solves that problem. Now we need vendors to build interfaces to those standards. Agencies have invested millions of dollars to equip themselves. We need to leverage these investments instead of replacing them.

Progress is already being made. DHS and DOJ are leading the development of emergency data dictionaries, models, and emergency message standards. SAFECOMM and related efforts are making significant progress on the radio interoperability front. As evidenced by NEARS and other developments, the leadership of a significant number of emergency professions has put their turf aside, in favor of cooperation.

A critical missing piece is a new idea, the need for a routing directory. Almost every one of the emergency warning systems has a different owner with different jurisdictions or geographical interests, different incident interests, and different electronic addresses. These differences have always existed, but the advancements in technology have created new questions. How does an agency send-

ing an alert know who the right organization is for public alerting in the target area, much less their correct computer address, incident interest, or geographic area of those interests? The answer is that no central entity can. That is why the shared registry, the emergency provider access directory, or EPAD, makes so much sense. If an organization wants to receive alerts and/or public warnings, either for itself or to pass on to others, it would simply need to register in the EPAD, with proper authorization. Instead of the inefficient creation of single-purpose directories, there should be one shared routing directory for all-hazards messaging, owned and managed on a nonprofit basis by the emergency-response profession.

We also need a similar shared rights-management system. What agencies are allowed to send alerts? What agencies are allowed to receive different types of alerts?

COMCARE has been working on these exact issues for more than 4 years. The result was a prototype of EPAD designed by teams of emergency practitioners and contributed by DICE Corporation. I would be delighted to schedule a time to show this to you.

Thanks to a major grant from the Department of Justice, we have run a series of national demonstrations using EPAD. We've funded the development of more than one-hundred pages of vetted final design and detailed technical architecture for both routing and rights management modules, and we have them right here today. We are ready to build the production version. The next step of the NEARS initiative is to obtain the funding.

NEARS is a unique plan to make a successful all-hazards alerting system possible. NEAR brings together leading emergency-response organizations around a common architecture and a specific plan, not a particular product. The detailed NEARS proposal is available on the Internet, at NEARS.us. The NEARS proposal provides for national demonstrations, building the production EPAD routing and rights management tools, and detailed beta field testing. It serves multiple missions, so it should be funded from multiple pockets of already appropriated funds. We believe it can move to a self-sustaining basis in 2 years, with interim Federal funding of less than $20 million.

The NEARS partner organizations have created a unique multiprofessional effort. We need your support to deliver on this promise for the American public. We request that Congress strongly encourage agencies to fund NEARS from already appropriated funds.

Thank you so much for your attention, and I'll entertain any questions.

[The prepared statement of Mr. Taylor follows:]

PREPARED STATEMENT OF RICHARD TAYLOR, EXECUTIVE DIRECTOR, NORTH CAROLINA WIRELESS 911 BOARD; CHAIRMAN, THE COMCARE ALLIANCE AND E–911 INSTITUTE; PARTNER, THE NATIONAL EMERGENCY ALERTING AND RESPONSE SYSTEMS INITIATIVE (NEARS)

Mr. Chairman and members of the Committee, thank you for the opportunity to testify before you today on this critical topic. There are few issues more important to our membership than the one you are discussing today.

COMCARE is a national non-profit alliance dedicated to advancing emergency response by promoting modern, interoperable emergency communications systems, and the development of new procedures, training, and tools to maximize value for emergency responders. COMCARE encourages cooperation across professional, juris-

dictional and geographic lines, and works to integrate the emergency response professions, government, private industry and the public. COMCARE's 100+ organizational members represent the wide diversity of the emergency response community. For more information visit *www.comcare.org*.

COMCARE's goal is to promote an integrated, coordinated approach to emergency communications and support the development of a comprehensive "end-to-end system" to link the public to emergency agencies, and to link those agencies together. Introducing 21st Century information and communications technologies to the often-antiquated communications infrastructure of emergency agencies will save thousands of lives each year, substantially reduce the severity of injuries, and enhance homeland security.

Our members have a vision of an integrated emergency communications and information system linking the public to emergency agencies, and linking the agencies to each other in a seamless network. This integrated network would equally serve to protect Americans during both daily and mass emergencies. The goal is to incorporate today's systems with tomorrow's technology under the cooperative guidance of local and national leadership.

I am also testifying on behalf of the National Emergency Alerting and Response Initiative (NEARS). Our NEARS partners include the American College of Emergency Physicians (ACEP), the American Public Health Association (APHA), the Brain Trauma Foundation (BTF), COMCARE, the Emergency Interoperability Consortium (EIC), the Emergency Nurses Association (ENA), the Fraternal Order of Police (FOP), the George Washington University Homeland Security Policy Institute (GWHSPI), the International Association of Emergency Managers (IAEM), the National Association of EMS Physicians (NAEMSP), the National Association of EMTs (NAEMT), the National Association of State EMS Directors (NASEMSD), the National Emergency Number Association (NENA), the National Volunteer Fire Council (NVFC), the Public Broadcasting Service, and others. See *www.nears.us*.

**Summary of Testimony**

We believe there are five essential building blocks for an effective, interoperable national public warning system.

- Interoperable pathways for agencies to exchange information
- Multiple communications channels from emergency agencies to the public
- A standards based system
- A series of shared Facilitation Services
- Use rules defined by emergency leaders and implemented through the Facilitation Services

Functional interoperability will not come from building a single new network, or multiple ones for specific types of warnings. There are close to 100,000 emergency agencies. There are hundreds of high quality communications systems in the emergency response and communications community now, and in the media. The physical networks to connect these organizations mostly already exist. We must take advantage of the extensive networks that are already in place and the tools that are used everyday by our emergency agencies. We should think of this as an "internetwork", and focus on connecting a wide variety of wireline and wireless networks that are controlled by a large number of separate entities.

This emergency internetwork will allow organizations to contact the public through all the burgeoning number of devices they have, not just one or two: wireless voice and data messaging, television, radio, beepers, ISPs, mass calling, and the like. Most discussions of public warning focus on this part of the process, the end point in the hands or living rooms of citizens. The COMCARE and NEARS focus has been on the other necessary pieces to make an all hazards system work.

Standards create a common language that enables data sharing between thousands of individual agency proprietary systems, and with the public. For public warning, the Common Alerting Protocol (CAP) standard fundamentally solves that problem, particularly when the EDXL Distribution Element becomes a standard as we hope it will later this year. Now the primary standards challenge is getting vendors to use them, to create interfaces to them.

The next issue is shared Facilitation Services. How does the sending agency know who the right organizations for public alerting in a target area are, much less their correct computer addresses, incident interests, and the geographic areas of those interests? Instead of the inefficient profusion of single purpose directories (and the inaccuracy that flows from such proliferation), there should be one shared routing directory system (actually a federated system of directories) for all hazards messaging, owned and managed on a non-profit basis by the emergency response professions.

The same comments and shared system apply to the needed rights management system. The Emergency Provider Access Directory (EPAD) NEARS and we advocate performs these routing and rights management functions.

Finally, it is important to separate technical capabilities from policy rules governing their use. Technically, we need a system that connects every emergency related organization together in the internetwork. That does not mean that any agency is allowed to send or receive any message or have access to any data. We need organizations at local, tribal, state and national levels to develop the policies and protocols that determine the rights and roles of agencies in the system, and management rules for it.

The National Emergency Alerting and Response Systems (NEARS) Initiative has a unique plan to make a successful All-Hazards Alerting system possible. NEARS brings together a wide variety of leading emergency response organizations around a common architecture and specific plan, not a particular product. With several regional and national demonstrations, using a prototype of EPAD (a map-based directory of agencies for routing data), we have proved that sharing data messages between agencies according to data standards is an extremely effective way to communicate with a wide variety of public warning systems. Thanks to a significant grant to COMCARE from the Department of Justice, EPAD has been specifically defined by teams of emergency practitioners, and an extremely detailed design has been created. We have more than 100 pages of design and a detailed technical architecture for both routing and rights management modules that are awaiting funding.

The 16 national organizations that are NEARS partners represent over 40,000 individual agencies and over 400,000 individuals in the emergency response professions. Our proposal serves multiple agency missions, from public warning, to emergency agency communications, to public health. We request that Congress strongly encourage DHS and HHS to fund NEARS from already appropriated funds.

**Overall Comments**

A public warning interoperability solution will not be achieved by the Federal Government purchasing a new national emergency alert network or buying a software application for the 100,000-plus emergency agencies—much less all the other public and private organizations that need to be part of an emergency network. Instead, emergency agencies and their communications capabilities should be viewed as a single "enterprise", with tens of thousands of agency owners. This enterprise needs to provide full interoperability among all agencies (and related organizations), delivering secure information and communication to/from response agencies and responders. It needs to include comprehensive public warning and education. To be cost efficient, it must be multi-user, multi-use, and all hazards.

The most effective public warning system will be one that gets emergency messages to the widest variety of possible alerting mechanisms ensuring that the greatest levels of penetration are achieved. It will be one that is used for all hazards reporting, not just tsunamis, or weather, or homeland security alerts. More importantly, it will be one that allows agencies to communicate directly with the public and those organizations authorized to send out disaster warnings directly to citizens. Finally, there will never be one "system" that solves the problem. We must have a capability that links all alerting solutions and allows for multiple methods of communication. That means it must be driven by data standards and based on an open architecture. It should not have single points of failure.

The National Emergency Alerting and Response Systems (NEARS) Initiative meets these criteria and can provide a solution to help our country achieve its goals. I am here today to ask you to support it as part of your broader, overall effort.

**The Problem**

Public warning rests on a simple action: some government agency needs to send out a warning. Sometimes this goes directly to the public; sometimes it goes to other emergency agencies or organizations for them in turn to notify the public. Sometimes the key targets of alerts are the individual employees of an agency or profession (*e.g.,* first responders, physicians).

In an era where technology can bring news, current events and entertainment to the farthest reaches of the world, to almost any electronic device, most U.S. emergency response agencies and personnel cannot share data with each other, even within the same jurisdiction, much less with the public they serve.

Most new cell phones can take and transmit pictures to any person on the Internet. If there were a small pox outbreak, it would be enormously valuable for CDC to be able to send pictures of pustules to 911, EMS, the media, and other key organizations so they could communicate them to the public. "If you have skin that looks like this, stay at home. Do not come into the hospital or contact others."

But most emergency response agencies cannot send or receive such data.

9/11 challenged the security of the United States and the safety of its citizens. Those challenges have identified weak spots in effective communication. Such emergencies demand real-time data and inter-operable communication across all jurisdictions and professional boundaries so that agencies can provide information and service to the public. There is an urgent need for broadband digital network capability for real-time, inter-agency, emergency communication, with seamless and effective communication capability from and to the public. Telephone and fax will not meet the need. Unfortunately, because we don't have standards or an open architecture, to achieve functional interoperable data communications today requires the construction of innumerable, specialized interfaces as demonstrated in Figure 1. Each of these interfaces needs to be replicated in every community. This is an unworkable model.

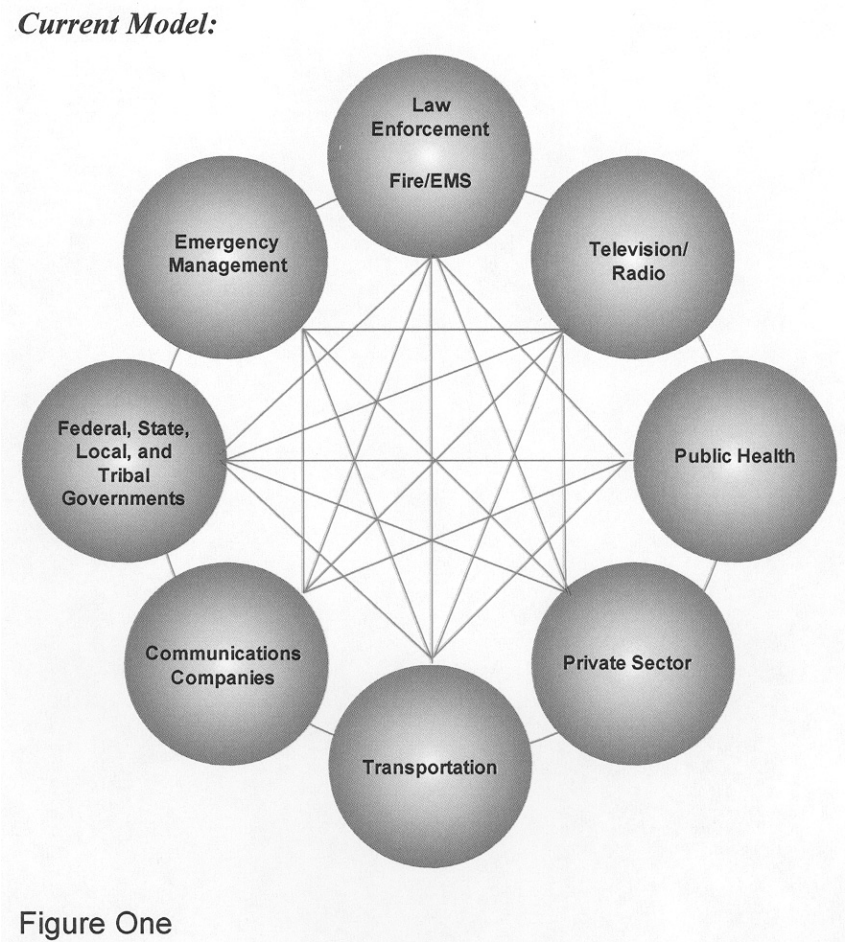



Figure One

It is simply impossible to achieve the National Incident Management System (NIMS) requirements for Communications and Information Management[1] without interoperable, interagency data communications. Yet today there are more than 100,000 emergency response agencies and the vast majority of them are not able to rapidly, accurately and easily communicate data with each other, much less the public. Except at the highest levels of government (*e.g.,* State EOCs and Governors that have been given data sharing tools by DHS), there is no regional or national

[1] NIMS Chapter 5.

emergency data communications capability. In simple terms, the President, the Secretary of Homeland Security, the Governor, or the EOC of any state, county, tribe or city do not have the ability to send or receive secure emergency messages to most of the more than 100,000 emergency agencies in our country or those in a particular state. Indeed, there is no comprehensive electronic directory of these agencies that would enable the routing of such messages.

Underlying this is a clear lack of a comprehensive local, State or national emergency communications and IT infrastructure. Most of the communications platforms used today are designed as one-off systems and solutions. The current system is voice-centric, and filled with stove pipes of information. There is little data sharing between agencies, much less with the private sector. Different agencies' information systems—computer-aided dispatch, emergency-management tools, public health applications, wireless data systems in the field, alerting and warning systems of all kinds—need to exchange up-to-the-minute information, but they cannot.

**Solution Overview**

Emergency responders are being asked to do one of the most important jobs in our society with generally the least advanced communications and information technology. The emergency community needs an integrated communications and information system for efficient preparedness, public warning, and response. This system needs to connect all emergency agencies with voice, data and video, not simply provide wireless voice and data connections to agency staff at the scene of incidents (which is a critical need). It also needs to connect the public to agencies and vice versa. The system needs to exploit the latest commercially available technologies, be highly secure, and provide emergency agencies with control over their data. Finally, we believe it needs to empower responders, giving them the flexibility to use emergency information in the ways they (not vendors or some central authority) choose, reflecting the different needs and capabilities of agencies in the communities of our country. Evacuating a town in rural Montana is quite different than evacuating Atlanta.

**Recent Progress**

There has been important progress in the last year. DHS and DOJ are leading the development of both emergency data dictionaries/models and emergency message standards. Project SAFECOMM and related efforts are making significant progress on the radio interoperability front. DHS and leading technology companies are supporting a range of data interoperability trials. A vision and plan for future emergency communications structure is emerging from the FCC's Network Reliability and Interoperability Council (NRIC) and similar proceedings. As evidenced by NEARS and other developments, the leadership of a significant number of emergency professions has put "turf" aside in favor of cooperation. These developments are new and incomplete, but encouraging nonetheless.

**Public Warning or Interagency Emergency Communications?**

Some draw a distinction between public alerting and interagency emergency communications. Certainly at a policy and specific use level, these can be different, but in general we do not think the two topics can be distinctly separated. Often at the state or local level the agency with information that needs to be communicated to the public (or the one with the tools that contact the public) is the state or local 911 center, police department or Emergency Manager. We must first make certain that emergency response agencies have the ability to efficiently receive and share emergency information of all types. Without that assurance there will be no accurate information to share with the public. We must also ensure that these agencies know who the right outlets are to notify the public and how to share information with them in real-time. As the train collision in South Carolina in January showed, this is usually not the case in complicated emergencies.

**What Systems Are Involved?**

Right now there are scores, indeed thousands, of emergency notification outlets to the American public. And they are generally controlled by thousands of independent emergency response agencies, few of which are connected to each other electronically (except by voice telephone). Here is a partial list.

- *Reverse 911 systems installed at or controlled by some of our 6,500 911 centers.
- *A wide variety of public individual notification registration systems (*e.g.,* D.C. Alert) in many of the 4,000 state, city and county emergency operations centers.
- Commercial registration warning systems (*e.g.,* some of the Amber Alert initiative; wireless company SMS systems).

- *Similar systems for senior officials (*e.g.,* RICCS and Roam Secure in D.C.).
- *Public Health Alert Networks from health departments linking physicians, hospitals, labs (*e.g.,* Virtual Alert in Virginia).
- *NOAA, National Weather Radio.
- Commercial and public media: TV, radio, cable, satellite.
- Non-traditional media: XM Radio, Sirius, Internet Service Providers.
- Wireless carriers; paging companies.
- *Specialized community warning systems (*e.g.,* around DOE and DOD facilities).
- *The traditional Emergency Alert System using broadcast systems.
- *DOT 5-1-1 and private traffic services.
- *DOT intelligent transportation public systems (*e.g.,* electronic road signs).
- Telematics suppliers and/or their customers (*e.g.,* OnStar and ATX).
- Internal corporate notification systems.

We have placed an asterisk next to the ones that are generally considered government emergency agencies—and might be initiating public warnings on their own, or because some agency like DHS told them to do so. We believe the definition of "agency" should include the entire above list, although the private ones would probably not be initiating alerts on their own). We also have over 140,000 schools—and they generally aren't on all hazards warning systems although some have weather radios now and they are now almost all connected to the Internet due to the e-Rate program.

**The Directory Problem**

Almost every one of the systems listed above has a different owner, with different jurisdiction or geographical interests, different incident interests, and different electronic addresses.

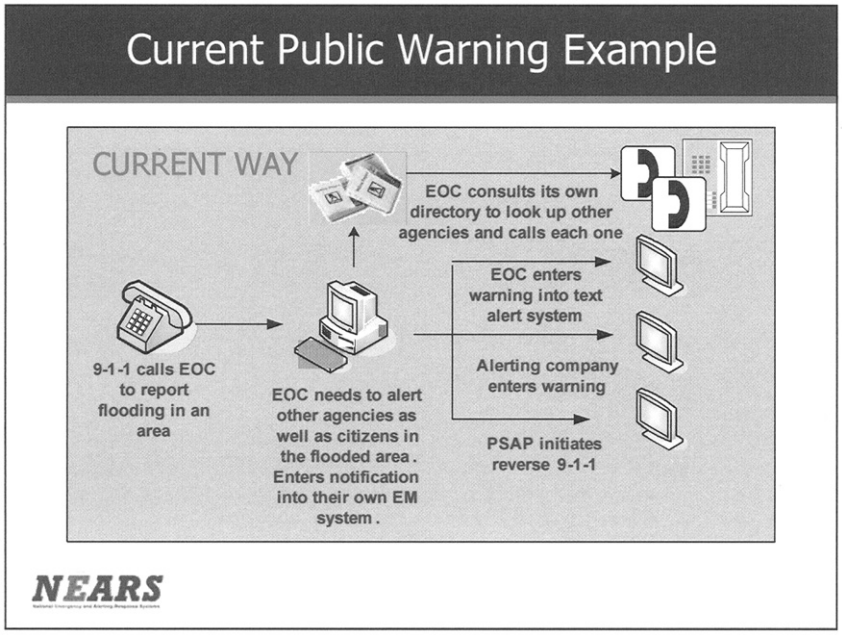
How are you going to find out that critical warning/alerting information distribution data and then keep it current? The answer is that no central entity can, local, state or Federal. That is why a shared registry where the organizations themselves enter this information—in other words, the EPAD we advocate—makes so much sense. If an organization wants to receive alerts and/or public warnings, either for itself, or to pass on to others, it simply needs to register in EPAD, and be authorized to do so. In about 10 minutes using a web interface, any such organization can enter what kinds of alerts it wants to get, for what geographic area, and delivered to what electronic address(es). Then any authorized messaging system can query the database and deliver the alerts.

Indeed, using the directory to enable (provide the addressees for) *all* emergency messages, not just the subset that are national alerts, makes it much more likely that agencies and other organizations will register and keep their information up to date—so that they can be reached by public alerts and warnings.

NEARS offers the ability to reach any organization (*i.e.,* the above list) that is registered to receive or disseminate a public warning message based on a geographic location. The detailed design of EPAD is done; it is ready to be built.

**Current Warning Procedure**

Let's look at a generic public warning message that does not originate at the Federal level.




911 receives a call about flooding in a large area that affects roadways, public buildings and a residential area. 911 calls the responsible emergency operations center (EOC) to notify them about the flood. It may also call other agencies.

The EOC determines that other agencies like traffic management and law enforcement must be called. The EOC enters the incident information into its system. It then looks up the telephone numbers for the agencies to be notified in its own directory—if it has one—and calls them one-by-one. It determines that a public warning message must be disseminated to those located in that area. However, it can only do so by using a zip code to target the message. Some may get the warning and are not affected. Others may not get the warning and could be affected.

Currently, the EOC uses three different systems to send out public warning messages—a text alert system, a voice alert system, and a website. The EOC enters the flood-warning message into each system so that warning messages can be disseminated.

The process involves making many phone calls and manually entering the incident message into each agency's system and each alerting system. The result—valuable time wasted, with an increasing possibility of message errors due to multiple manual entries.

For there to be an effective public alerting system there must be only one communications system for all events. One system should be created to contact the public for all events, ranging from child abductions, to hurricanes, to terrorist attacks. Having multiple systems for different types of alerts is wasteful because it creates several systems which have a limited range of contact, instead of creating one, all-inclusive system. One system will allow all registered agencies and organizations to send and receive messages about any event.

Saying that there should be one system, does not mean there should be one set of rights, one set of use protocols, or any similar capability which is unique to an incident type. The point of Facilitation Services is to have electronic tools that allow those different capabilities and rules to be implemented.

**Essential Parts of a National All-Hazards Alert System**

There must be one system for all warnings, not one for each kind. There are tens of thousands of alerts that are sent to emergency agencies, the media, and the public each year, and there are thousands of agencies who are responsible for reporting these warnings. Cellular phones, Internet, CAD systems, text messaging, beepers, television, radio, cable should all be used for public alerting. The technology exists to create this integrated alerting system.

There are five essential building blocks or layers for an effective interoperable national emergency communications system; they are the same for a national public warning system. Some of these layers will be provided on highly competitive terms by multiple parties, some are shared Facilitation Services offered by collections of emergency response agencies, while others are components that will be unique to individual agencies:

1. Pathways for agencies to exchange information.
2. Pathways from the agencies to the public.
3. Emergency communications standards.
4. A set of shared Facilitation Services for routing, rights management, security and the like.
5. Institutions to define rules and policies.

*1. Interagency Communication*

For a successful integrated public warning system to exist there must be interoperable communication between agencies. Local 911 centers, HSOC, NOAA, FEMA, and emergency responders should be linked by an alerting network that allows these agencies to receive and disseminate the information they need as quickly as possible. We don't need to build a new network. Commercial telecommunications entities, and state and local governments, have already deployed massive fiber, satellite and wireless infrastructures. We need to assume an "internetwork", connecting a wide variety of wireline and wireless networks, controlled by a large number of separate entities.

This can be the public Internet; that has the advantage of being available to almost any agency immediately, and for very low cost. However, many localities and states have developed their own private IP networks; these provide better performance. The primary policy issue—and one that is very familiar to this Committee—is getting all emergency agencies to establish broad band connections.

*2. Standards*

Standards create a common language that enables data sharing between the thousands of individual agency proprietary systems. It is no solution to require all agencies to use the same information technology tools. Most agencies will not be willing to let someone else make these decisions for them, nor will they be comfortable or efficient using tools that they do not use on a daily basis. The costly alternatives are to develop individual interfaces for each source of data, or to acquire complicated and expensive systems that sit between agencies and translate each agency's data language into the others.

Common standards allow data communication among the disparate systems that are already in use, along with new applications as they are introduced into the system, by essentially building a single interface for all such purposes.

Standards have to be national. National standards mean local and state technology choices will expand and prices should improve, following the experience of the private sector with the commercial computer industry. It is equally important that representatives from the full range of emergency response professions be at the table during the national standards development process.

The Department of Homeland Security (DHS) through OMB's Disaster Management eGov Initiative identified the need for data interoperability using common standards. DHS is facilitating a process, in which COMCARE is proud to be a partner, that brings together leaders of the emergency professions that need to share data during emergency response operations. The project is developing and field testing a common set of emergency message standards (the Emergency Data Exchange Language, EDXL). It is also supporting broader efforts to develop common data terms and models, specifically the National Information Exchange Model (NIEM) project, that is based on the excellent pioneering work of the Global Justice XML Data Dictionary and Model. We strongly support these efforts, and are using these standards in NEARS and our other demonstrations.

*3. Communications to the Public*

To get to the public, you first have to get the alert to emergency agencies and other organizations (*e.g.,* the media). Agencies and organizations will receive alerts and warnings on a wide variety of information technology tools before they can decide to (or automatically) re-transmit those warnings to the public each serves. There are numerous emergency applications in use today, including complex Computer Aided Dispatch Systems (CAD), web-based emergency management tools, alerting systems for notifying emergency staff, mass residential communications systems, and other applications. Each of these systems has their own unique

functionality; agencies should be encouraged to purchase the tools that are best suited for them. However, it is critical that these applications all have a standardized interface: the ability to send and receive XML messages to other applications in standardized formats. When 911 is in charge of public alerting, it should not matter to a 911 CAD system that it is receiving data from an emergency management tool about a flood, a bioterrorism alert from CDC, or data about a 911 call from a wireless company. The same data interface should be used. That is what the standards are all about.

Another set of applications and services are those that compete to deliver information from these agency-based applications to the public. These can range from traditional ones that provide links through landline telephones, radio, or data connections, to NOAA weather radios, to beepers, warning radio systems, and even the traditional sirens. Broadcast television, radio, cable, Internet service providers and others provide other outlets to the public. In some cases these are linked to more sophisticated systems which enrich incident messages with associated data from multiple sources.

Much of the debate about public warning has tended to revolve around the issues of consumer devices: which is "best"? Should there be mandates?

We believe that public warning is today like a doughnut. There is a lot of capability at the edges where the vast array of systems touch the public. There is a large hole in the middle. Our preference would be to focus on filling the whole, making warnings available in standardized forms to all these outlets as appropriate, and then see what other steps need to be taken.

*4. Facilitation Services*

"Facilitation services" are shared tools, services and/or resources that are offered by collective effort of the emergency response community, and are available to authorized emergency entities to enable interoperability. These include, but are not limited to, security, diagnostics, routing directory, agency rights management, data rights management, and authentication.

Without a directory of agencies and their electronic addresses, public warning messages cannot be routed. Rather than the inefficient profusion of single purpose directories that is growing today, we believe there should be one shared directory system, owned and managed by the emergency response professions. This should be a secure registry where authorized agencies enter their name, contact information, professional function, level of government, incident interests (and the geographical area of both jurisdiction and interest for each type of incident), and emergency data delivery address(es). Only authenticated and authorized agencies will have access to it on a non-discriminatory basis.

Authentication and rights management are critical as well. There must be a trusted way to credential agencies and individuals, provide them with appropriate authorizations (both sending and receiving), and allow them access to and use of the network. Linking networks will require systems that will assure only authorized parties may participate, assign them appropriate rights and roles, and authenticate communications from them. Rights management also needs to be applied to data itself.

COMCARE has been working on these exact issues for more than 4 years. The result is the Emergency Provider Access Directory (EPAD). A routing prototype developed as a contribution to the public interest by our member DICE Corporation is available at *http://www.epad.us*. We are using this in field trials and demonstrations all over the country.

Thanks to a major grant from the Department of Justice the EPAD concept has been advanced a long way. There is now a detailed design of the production version of EPAD. More than 100 pages of design and a detailed technical architecture are awaiting funding to do the coding. This will provide both routing and rights management modules.

*5. Policies and Protocols*

It is important to separate technical capabilities from policy rules governing their use. Technically, we need a system that connects every agency together in a network. And the word "agency" must include many private sector entities. But that does not mean that any agency should be allowed to send or receive any message or have access to unregulated data.

COMCARE believes that emphasis should be placed on system flexibility, and local control, using the rights management Facilitation Services to allow for messages to be generated from local and state emergency managers (to their appropriate audiences) as well as national sources. After all, most emergencies are local.

We need to develop the policies and protocols that determine the rights and roles of agencies in the system, and management rules for it; a local 911 center should not have the same access within the system as a Governor. Some of these policies (and the decision-making bodies) are already in place today, whether they are officially written policies or not. Many are not, and most lack all the parties they need to be effective in this regard. The local, state and Federal law enforcement communities are most advanced in this regard. Most other emergency agencies are not involved because sharing emergency information between them has not been done before. All of these policies and protocols will need to be addressed in terms of electronic communication.

Applying this architecture results in a very different approach than Figure One. Figure Two shows a more rationalized system where appropriate functions are shared.

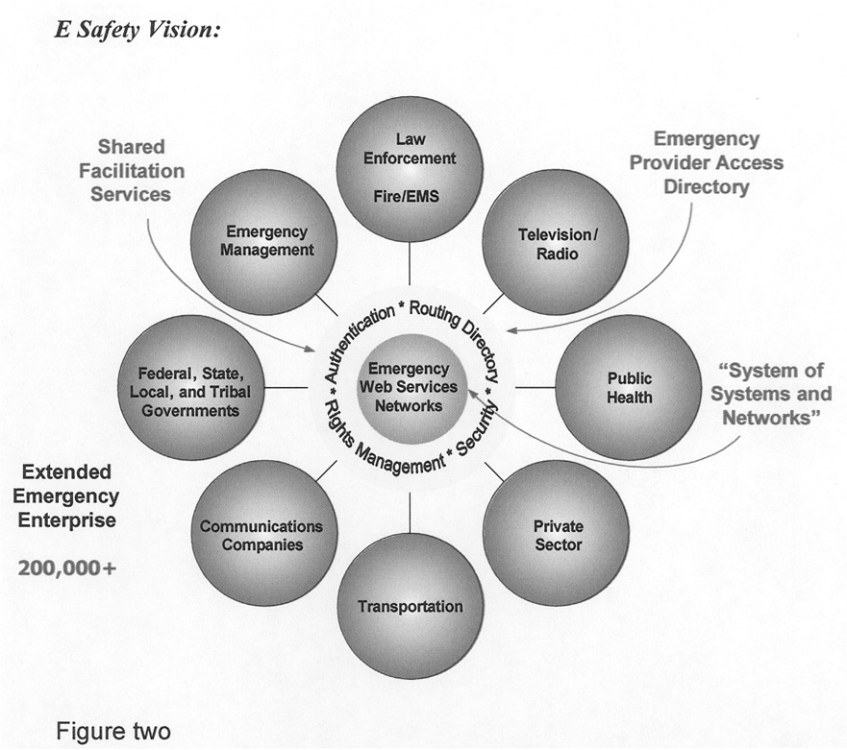



Figure two

**NEARS**

The National Emergency Alerting and Response Systems (NEARS) Initiative implements national emergency message standards, commercial information technologies, and the EPAD shared, electronic directory of agencies being developed by a non-profit public/private partnership.

NEARS is endorsed and led by a growing and diverse coalition of emergency response and industry organizations. Participation by others is actively encouraged. It is a three-track initiative that promotes the concept, develops the service, and tests the service for national implementation with actual deployments in several regions.

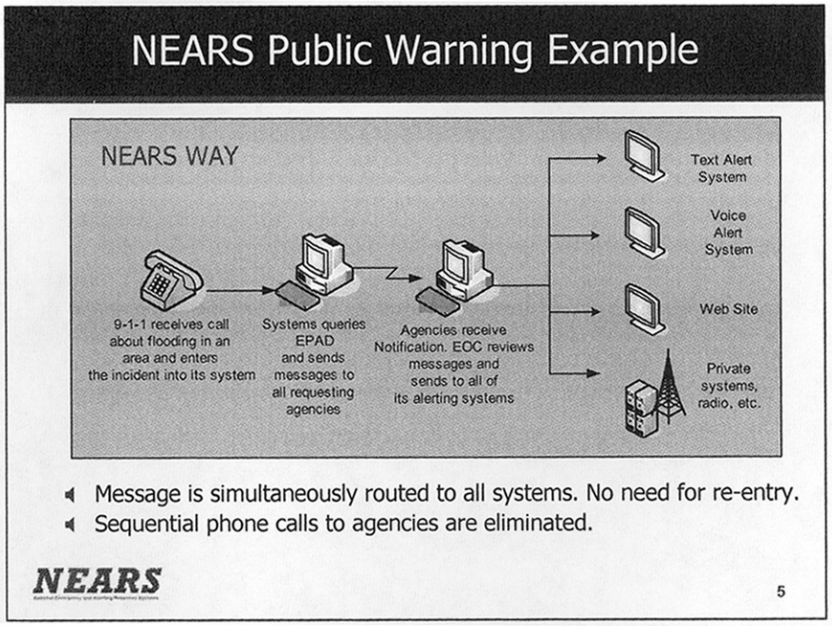
NEARS was created to bring together the respective players in the emergency alerting area, and to provide a forum for government, industry and other interested parties to work together to improve the Nation's public warning and emergency messaging capability. Together we plan to demonstrate and deploy interoperable emergency data messaging, using national emergency message and data standards, commercial information technologies, and the EPAD shared, electronic directory of agencies. This directory gives agencies the ability to distribute emergency messages based on geography, incident or agency type, for all types of emergency events.

Our NEARS partners include the American College of Emergency Physicians (ACEP), the American Public Health Association (APHA), the Brain Trauma Foundation (BTF), the ComCARE Alliance, the Emergency Interoperability Consortium (EIC), the Emergency Nurses Association (ENA), the Fraternal Order of Police (FOP), the George Washington University Homeland Security Policy Institute (GWHSPI), the International Association of Emergency Managers (IAEM), the National Association of EMS Physicians (NAEMSP), the National Association of EMTs (NAEMT), the National Association of State EMS Directors (NASEMSD), the National Emergency Number Association (NENA), the National Volunteer Fire Council (NVFC), the Public Broadcasting Service, and others.

Some criticize responders for only communicating within their professional silos. However, the growing number of organizations who support NEARS clearly demonstrate that there is willingness to change. Collectively, the NEARS partner organizations represent a large cross section of the emergency response community—Law Enforcement, Fire, EMS, Public Health, 911, Emergency Management, and the media. We do not have all the groups we want, but the current partners represent over 40,000 individual agencies and over 400,000 individuals in the emergency response profession. This is a solid foundation and the initiative continues to add partners. We hope you will strongly encourage DHS to fund this project, providing the ability for emergency response organizations of all types to share information amongst themselves and with the public during emergencies. It serves a variety of homeland security purposes.

The NEARS partners seek to attract involvement from all the leadership groups of these professions and from additional segments such as hospitals, transportation, state and local government and keep it growing.

Once NEARS is deployed, this is how this same scenario would play out.




911 receives the call and enters incident information into its system and requests that the message be sent to all appropriate agencies in the area. The 911 system then queries EPAD and using an EDXL Distribution Element sends a CAP message to all agency addresses that are returned.

The message is entered once—into the 911 system and disseminated electronically to all appropriate agencies as well as to the public alerting systems if the EOC elected to do so. The EOC can then schedule public dissemination once the message is reviewed and approved. The whole process is quick and efficient and the public is notified in time for them to react—no phone calls, no multiple entries, no errors.

When a user or other entity initiates a login or message, EPAD Identity Rights Management authenticates it and indicates what privileges are allowed.

If the user and/or system or device is allowed to create and send an incident message, the message can be created and EPAD can be queried for instructions as to where to send it. The system or device can query EPAD directly or it can use a message broker service that will query EPAD and disseminate it for the entity. In either case, a web service query is sent indicating the type and time of the incident, where it occurred and, if applicable, what types of agencies should be notified. EPAD will search the directory to determine the entities that requested this type of information. It will send back a list of all entities indicating how the entity wishes to be contacted. It can be a system to system transmission, an automated phone call to certain individuals and/or other types of contact.

The system or message broker then sends the message to all entities simultaneously. If the user and/or entity is authorized to do so, it can review the list first and make changes to the distribution list before dissemination.

**Public Broadcasting**

A special word about public broadcasting is in order. I am delighted that they are represented at this hearing.

Public broadcasting can play a critical role in emergency preparedness, emergency communications and public warning. As John Lawson of APTS has testified, there have been successful experiments in data casting using digital capacity of stations and the PBS interconnection. We commend APTS and DHS for those forward thinking trials. We encourage the proliferation of this capability. But to limit public broadcasting to this role would be to give up some critical strengths it can offer. In addition to whatever data casting capability public broadcasting might have in the future, we should take full advantage of three unique attributes it can offer us today:

- Network capacity provider: PBS has a national backbone digital satellite and terrestrial network reaching every state and significant community in the country.
- Local television and radio signals reach out from that core network to cover over 99 percent of Americans.[2]
- Public broadcasting is made up of trusted and respected local and national public service organizations that could be a "Switzerland" in bringing together all the relevant parties.

PBS is a NEARS partner. We think PBS could be a national leader in convening the coalition partners to identify the connectivity and interconnection requirements locally, regionally and nationally of the various agencies and organizations. Second, PBS would work in collaboration with the initiative partners to incorporate agreed to standards, routing and authorization applications, data messaging formats and any necessary trial/pilot demonstrations. The NEARS Initiative is exactly such a nonprofit public service coalition project.

**Conclusion**

The detailed NEARS proposal is available at *www.nears.us.* It is based on the important investment by the Justice Department in EPAD, and the DHS investment in common emergency messaging standards. The NEARS proposal provides for national demonstrations, building production quality EPAD routing and rights management tools, and detailed beta field testing of them. Because it serves the missions of multiple government agencies, it is the priority of none of them. Because it serves multiple missions, it can and should be funded from multiple "pockets" of already appropriated funds. We believe it can move to a self-sustaining basis in 2 years, with Federal funding of less than $20 million.

Thanks to the leadership of my colleagues from the other NEARS partner organizations we have created a unique, multi-professional effort. We have overcome the turf concerns. We need your support to deliver on this promise for the American public.

Senator DEMINT. Mr. Guttman-McCabe, let me ask you a question. One of my concerns in this process is, we'll come up with mandates, for instance, that wireless services will have to broadcast a

[2] Beyond pure technical contributions, we just recognize that public broadcasting is made up of respected and "neutral" local station organizations directed by community leaders; a similar national organization which can play a convening role in the key public and private partnerships needed. They also have highly experienced and successful local and national programming capabilities which can be used to build training and other content for alerts.

message. And, you mentioned that wireless servers, like the one I have for this, are not set up to broadcast, so we'd have to change their technology in order to do that. I'd like to make sure we have thought of other options. And my question, just a technical question—this is designed to receive a signal from only one server. Is there any way this could be easily adapted so that, in an emergency, that it could receive, directly, a signal from public broadcasting digital, and not even go through the central server that it's designed to pick up from?

Mr. GUTTMAN-MCCABE. Mr. Chairman, let me answer that with a strong caveat that it would probably be beyond my technical expertise. But I—the systems, I think, are designed—and the handsets, whether it be a BlackBerry handset or a wireless handset—are designed to be operational solely with that wireless provider.

Senator DEMINT. Right.

Mr. GUTTMAN-MCCABE. So, our industry is made up of different technologies and different platforms, and, even within those platforms, there are different generations of technologies. That's part of what makes moving forward with an emergency alert service a difficult concept, a difficult process.

Senator DEMINT. Well, do you think there will need to be a Federal mandate that wireless companies cooperate, that they all basically do the same thing in order for there to be cooperation from the wireless industry?

Mr. GUTTMAN-MCCABE. Mr. Chairman, I would say that I think we would support exactly the opposite contention, that if left to the ingenuity and the creativity of the industry, you're going to get a solution that makes most sense with the existing technology, but also that recognizes that there will be an evolution in the networks. And I fear that if something were to be mandated—and I think you, in the earlier panel, stated such fears—I fear that government could get it wrong and that a choice could be made on a technology that, by the time the process is developed and the standards are developed and the equipment is developed, it's already a generation behind what actually exists.

So, I think I would—the industry, I think, would wholeheartedly support a voluntary effort and a cooperative effort with government.

Senator DEMINT. Senator Nelson?

Senator BEN NELSON. Maybe any one of you could respond to the concern with the 100,000 agencies and the potential of multiple warnings instantaneously around the country. At what point do we run the risk of an overload? Is the capacity—that you currently have from public broadcasting—capable of receiving such warnings from so many different locations and then disseminating them?

Mr. LAWSON. Senator, we have the capacity even to do video through—this is all browser-based, this is Internet protocol—even to do video requires just a fraction of what we have. I think the——

Senator BEN NELSON. But if you have multiple warnings—I doubt that you could have 100,000—coming from all at one instant in time, would there be an overload point for the technology?

Mr. LAWSON. Since we're talking about regional, for a local public television station, there is a limit to what we can put over the sat-

ellite, certainly, but you wouldn't have 100,000 coming in to us—one public station. You might have a dozen or so agencies. The real question is the overload of information that the public receives.

Senator BEN NELSON. Well, that's a given, yes.

Mr. LAWSON. Right. So right now, under the analog EAS, we and the other broadcasters do have a responsibility to pass along Presidential messaging in the event of a national emergency, but there is a voluntary system in place, in terms of what is carried from local and state governments. And I think one of the challenges we face is to work out the protocols, we, in FEMA, are planning to roll out a national Federal alert system. The challenge of connecting local and state emergency managers to that system, to that backbone, to use local stations, is partially financial, but it's also working out the exact kinds of protocols I think you're alluding to, in terms of what is emergency data, what is emergency information, and what is our responsibility to pass it on, on a metropolitan-wide basis, if it's only affecting a certain part of the community.

Senator BEN NELSON. What about security? In other words, with the advent of so much information, the potential for warning information to be put out in alerts, what kind of assurance can we have that will be authorized, that you won't have the equivalent of spam or people intervening and putting out their own misinformation?

Mr. LAWSON. Well, I can tell you, in our situation, we're looking at a dedicated communication link between FEMA and our satellite system of the local station transmitter. That has to be secure, and it has to be hardened. And I'm sure that will be part of the rollout. But in terms of what leaves the station, what leaves the transmitter, in terms of over-the-air, it's pretty much unhackable at that point. And we can encrypt it, so that only certain people, authorized users, can have access to that information.

Senator BEN NELSON. Therefore, the chances of an April Fool's joke is probably remote or nonexistent.

Mr. LAWSON. In the system that we're testing here in the national capital region, yes, sir, I think it would be pretty difficult.

Mr. GUTTMAN-MCCABE. Senator, that is a concern of ours, and it's something that we think—we agree, that is being worked. And part of the process of working with FEMA and Mr. Hoover is getting to a policy and a process whereby—as Mr. Hoover mentioned, whereby messages are originated, at some point, and then not touched as they move throughout the process. So, when they move through a wireless network, we—our industry understands that it has not been corrupted, it's not corruptible, it has been authenticated, and that no one on the wireless side has to touch the message. And I think that is a key concern and a key element of any network, going forward.

Senator BEN NELSON. So, it wouldn't be as amateurish as the signals between the pitcher and the catcher in a baseball game.

[Laughter.]

Mr. GUTTMAN-MCCABE. One would hope not.

Senator BEN NELSON. All right. Thank you.

Senator DEMINT. I think you were here to hear the first panel. I'd be interested in your comments. We're completing legislation at this point. I have a new sense of urgency to complete it and get it passed, because it's going to be a rush to get it done before the

FCC completes their rulemaking, without the legislation, apparently. But based on what you heard, what are your concerns about the rulemaking, about the legislation, or what would you like to make sure that we include in this? And I'll just ask each of you to give just a very brief comment before we close.

Mr. GUTTMAN-MCCABE. Thank you, Mr. Chairman.

You have voiced, actually, some of our concerns, the concern that a technology choice will be made, or that a date certain will be set that doesn't make sense, in terms of development of a solution. That's why CTIA and the industry have approached this with a two-part solution, the first part being working with FEMA on the pilot project, utilizing an SMS-based solution, existing technologies, sending a text message to devices, and utilizing an opt-in service, but also simultaneously looking at some longer-term solutions that address issues like capacity and the ability to target messages geographically. So, I would be concerned and would want to ensure that any legislation, from our perspective, would recognize those limitations.

Also, addressing issues such as an actual description of what the service should be. It's difficult for manufacturers to build a technology to a service that they don't know exactly what the parameters are, of yet. Again, who can send a message? When can they send a message? What should the message contain? Does it contain data? Does it contain pictures and maps? How quickly does it have to be disseminated, and to whom?

So, all of those things will inform the standards groups, and the standards groups will turn around and develop standards by which the manufacturers can build equipment.

So, this is a process that actually is ongoing, much like Mr. Hoover and their effort to develop a coordinated government effort. These efforts are ongoing, and we would hope that any legislation wouldn't, sort of, either short-circuit that process or derail it in a way that actually harmed the actual development of a service.

Senator DEMINT. Mr. Taylor?

Mr. TAYLOR. I come from a rural area of Eastern Carolina that's had its share of hurricanes, but it also has its share of 911 centers that have invested what little bit of money they have into systems that they feel like they can work with, that they can afford. Our concern is that we don't need to go out and build new wheels; we have wheels that work right now. We have rural areas, we have PSAPs, we have emergency managers that are using notification systems that fit their budgets, that fit their needs. And we're not wanting to change that. We want to interface all of those different systems, instead of going out and rebuilding a whole network. Let's take the networks that we have today, and let's create standards of interface. And that's what we would encourage, is that, let's work on the standards for interfacing all the different systems that we have. Interface the BlackBerrys, interface the wireless carriers, interface the public television system, interface NOAA. All these different emergency notification systems are wonderful, they work great. We're not trying to rebuild the dots, we're just trying to draw the line between the dots. And that's what we're concerned with. We don't want to rebuild a good system. We want to take what we have and make it able to talk to each other, able to communicate

with each other, without having to spend millions and millions of dollars replacing what's already there.

Senator DEMINT. Mr. Lawson?

Mr. LAWSON. Mr. Chairman, with public television we're talking about a classic dual-use opportunity. And our stations have raised about 1.1 billion to convert to digital, which was a subject of the full Committee's hearing a couple of weeks ago. Most of that's non–Federal. To use a system as the backbone for a Federal emergency alert system requires an incremental investment, and it requires the continuing maintenance of the infrastructure that we have. So, in our testimony we're asking the Committee to continue to support, the rebuilding of our satellite interconnection system, which is getting old and has to be replaced. And, second, FEMA is handling the national Presidential-messaging part of our system from their own resources, but to take—to provide resources for national and local connection to this backbone, for national and local origination, for messages of that level, extra funds are required, and that would be our request.

Senator DEMINT. Thank you. This has been most helpful. I appreciate everyone being here, everyone in our audience and the media.

This hearing is adjourned.

[Whereupon, at 11:30 a.m., the hearing was adjourned.]

# A P P E N D I X

PREPARED STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

Mr. Chairman, thank you for holding this hearing today. In the aftermath of the deadly Indian Ocean tsunami, we in the Senate, like so many around the world, asked two simple questions: "Why couldn't we warn people that this tsunami was coming?" and "Would we receive an adequate warning if a disaster happened here?"

Unfortunately, the issue of effective warnings is more complicated than it seems at first blush. As we have learned over the course of the year, there are several elements to an effective warning:

1. It must detect or predict the hazard;
2. It must communicate the warning to those in danger; and
3. It must offer sound advice on how to find safety.

Our witnesses today are likely to focus on the second problem—getting the warnings to affected people. Coordination and the use of new technologies are very important. However, I would like to urge our witnesses not to forget the other two pieces of effective warnings. We need to invest in improving our detection and prediction of all hazards, including tsunami, volcano, earthquake, and weather hazards. In addition, we must ensure that people know what to do when they are warned. That means that Federal, state, and local governments need to have a coordinated response and need to educate at-risk communities on how to respond to natural or man-made disasters.

With regard to communicating warnings to those in danger, I am excited to hear about new, off the shelf technologies that can improve and personalize warnings.

Particularly in communications-saturated cities, like Washington, D.C., these technologies can help spread the word quickly and effectively.

Of course, many places in this country, particularly the Western Pacific, lack ubiquitous telecommunications. In these places, we must focus on deploying robust, low tech solutions like sirens or radios on a stick that can deliver warnings where they are needed.

NOAA, FEMA, and the White House have established a task force on effective warnings under the auspices of the National Science and Technology Council. The task force is working to improve both natural disaster and homeland security warnings.

As you continue integrating the various Federal systems, I encourage you to involve a variety of state and local emergency managers and first responders to ensure that we preserve our existing capabilities at NOAA with respect to warnings for weather and other natural disasters; we improve, rather than interfere with, access to such warnings by local emergency managers and first responders; and we develop and deploy technologies appropriate to each community.

The United States can do better at warning its population. I look forward to hearing our witnesses help us find a way forward so that we can make people throughout the Nation safer from whatever hazards threaten us.

○