PPW Report 2003-01

PARTNERSHIP FOR PUBLIC WARNING

A National Strategy for Integrated Public Warning Policy and Capability

Partnership for Public Warning

February 2003

7515 Colshire Drive MS N655
McLean, VA 22102
TEL: (703) 883-2745
FAX:(703) 883-3689

The Partnership for Public Warning

The Partnership for Public Warning (PPW) is a partnership between the private sector, academia, and government entities at the local, state and Federal level. PPW was incorporated in January 2002 as a 501(c)(3) public/private non-profit institute, the type of entity recommended in the report *Effective Disaster Warnings* authored in 2000 under the National Science and Technology Council at the White House (www.nnic.noaa.gov/CENR/NDIS_rev_Oct27.pdf).

PPW's mission -- To develop consensus on processes, standards and systems that will provide the right information about dangers to life and property to the right people, in the right places, and at the right times, so those in harm's way can take timely and appropriate action to save lives, reduce losses and speed recovery – whether from natural disasters, accidents, or acts of terrorism.

PPW's Vision -- For every person to have the information needed in an emergency to save lives, prevent injury, mitigate property loss, and minimize the time needed to return to a normal life.

www.PartnershipForPublicWarning.org

Background on this Report

A primary goal of the Partnership for Public Warning is to develop consensus on a national vision and specific goals for improving all-hazard warning systems at the Federal, state and local levels. To seed this process, PPW sponsored a workshop that was held during December 4 - 8, 2002, at the Emergency Management Institute in Emmitsburg, MD, to develop the first draft of a National Strategy. In attendance were knowledgeable representatives of many of the stakeholder groups concerned with public warning. Participants are listed in Appendix 1. This draft is being circulated widely to stakeholders for review and comment. We hope in this way to develop national agreement on vision and goals. People who have reviewed and commented on this report to date are also listed in Appendix 1.

IMPORTANT ANNOUNCEMENT

This document is a draft provided for your review. Does this national strategy describe the national need as viewed from your perspective? Are there topics that are not covered and need to be discussed? Are there issues with which you disagree?

Please read this document carefully and send any comments with a brief description of your stake in these issues to:

stratplan@PartnershipForPublicWarning.org

The Partnership will modify this draft based on input received before April 18, 2003, and will compile separately all comments received. The final National Strategy will be released in May 2003.

Executive Summary

Public warning empowers people at risk to take actions to reduce losses from natural hazards, accidents, and acts of terrorism. Public warning saves lives, reduces fear, and speeds recovery. Its success is measured by the actions people take.

Warning is an important element of providing for public safety. Public safety is a fundamental duty of municipal, county, and tribal government and, for larger hazards, of state and Federal government. Public safety is also the responsibility of citizens to take action not only to protect themselves and their loved ones, but also to make society safer through their jobs and community activity.

The American people believe that a public warning system exists. While current warning systems are saving lives, they are not as effective as they can be or should be. This document explains the problems with our national warning capability and charts a course for providing what the American people need and expect.

The National Weather Service issues the majority of public warnings in the United States and has developed sophisticated warning procedures and systems. The National Oceanic and Atmospheric Administration (NOAA) Weather Wire System operated by the Weather Service and the National Warning System operated by the Federal Emergency Management Agency (FEMA) provide ways to collect and distribute warning information to emergency managers and other key personnel nationwide. The Emergency Alert System and NOAA Weather Radio provide ways to deliver warnings to some of the people at risk. A wide variety of other warning systems reach people at risk around critical facilities such as dams, chemical plants, oil refineries, and nuclear facilities. Many private businesses will deliver warnings to subscribers through telephones, wireless devices, and email.

A basic problem with current public warning systems is that they do not reach enough of the people at risk and often reach many people not at risk. Few local emergency managers or first responders have effective ways to input information and warnings into these systems. Warnings from different sources are rarely available to all warning systems in a given region. Many of the systems are not interoperable. There are very few standards, protocols, or procedures for developing and issuing warnings. Warnings from different sources use different terminology to express the same issues of risk and recommended action. Even the national Emergency Alert System has increasing inconsistencies and potential points of failure due to decreased funding and failure to develop state and local plans for proper utilization.

All stakeholders involved in public warning should be represented in developing an effective national public warning capability. The Federal government needs to provide leadership, but cannot do it alone. The primary responsibility for warning resides with county, municipal, and tribal government, but they often need state and Federal assistance. Scientists, intelligence experts, and other authorities develop warning information on regional, national, and even international scales. The news media relay and explain warnings, and the broadcasters and cable operators operate the Emergency Alert System. Industry plays a key role in developing,

building, and operating warning systems. Certain industries also provide public warnings around critical facilities. Many professional and trade associations as well as non-profit organizations and volunteers represent the needs of various groups involved in delivery or utilization of warnings.

Our national warning capability needs to be focused on the people at risk at any location and at any hour, be universally accessible, safe, easy to use, resilient, reliable, and timely. Numerous technologies exist to do this and in many ways technology is the easiest part of the solution. The bigger challenges are to provide accurate, understandable, specific, and informative warnings and to develop procedures and processes for collecting and disseminating those warnings in standard and secure ways.

For warnings to be readily available to all people at risk, no matter where they are or what they are doing, the warning capability should be ubiquitous, but in an unobtrusive manner that respects privacy and individual choice. This requires partnership and teamwork among all the different stakeholders. An effective warning strategy must enable industry to develop a wide range of market-based solutions. Industry needs a clear statement of government intent and clearly articulated standards that specify required interoperability for a national warning capability. Industry will be naturally motivated to augment basic interoperability with competitive capabilities and refinements.

States, counties and municipalities have developed disparate alert networks at a cost of hundreds of millions of dollars; these networks are not particularly effective, are not interoperable, and will be difficult to consolidate. To alleviate this massive duplication of effort and waste of money, national policy should be adopted calling for partnership in linking all stakeholders and the public with this imperative community-specific information. The partners need to develop the policies for and implementation of a national warning backbone that will provide to a wide variety of warning delivery systems all public warnings for any region utilizing standard terminology and procedures. Such a capability should leverage existing and developing public and private network capabilities.

The President and Congress need to make public warning a national priority, assign lead responsibility to the Secretary of Homeland Security, appropriate the necessary funds to engage the appropriate stakeholders effectively in developing national standards and protocols, and set deadlines for implementation. Public warning should also be made a priority for other federal programs so that information is gathered in a manner that will support this endeavor.

Working together in partnership, the stakeholders should assess current warning capability, carry out appropriate research, and develop the following:

- A common terminology for natural and man-made hazards
- A standard message protocol
- National metrics and standards
- National backbone systems for securely collecting and disseminating warnings from all available sources

- Pilot projects to test concepts and approaches
- Training programs
- A national multi-media education and outreach campaign

If we act now, each and every American at imminent risk can have immediate access to warnings, knowledge of how to take appropriate action, and a choice on selecting what information is delivered and under what circumstances. Although this document deals with national strategy, we feel it is important to estimate initial costs required to bring it to fruition. A significantly improved national public warning system can be up and running within two years, at a Federal outlay of no more than $15 million annually. Once that happens, it is not anticipated that large amounts of Federal funding above current levels will be either required or appropriate, as an important advantage of this strategy is that most federal government costs are up front … to prime the pump.

Many key stakeholders are already making an investment and effort, and have laid the groundwork for a federal authority to step up to the challenge. We all have a shared duty and obligation to act. September 11th taught us that the unthinkable is no longer an excuse for delay. Future tragedies are not a matter of if, but when. Lives can be saved and losses reduced through effective public warning. Americans expect their government to protect them and believe an effective warning capability exists. However, an effective warning capability does not exist, and it is only as matter of time before our nation will come to wish it did.

National Strategy for Integrated Public Warning Policy and Capability

Critical Need For Public Warning

Public safety is a fundamental duty of municipal, county, tribal, state, and Federal government. A significant portion of government's energy and budget is spent on identifying hazards and creating standards and laws to reduce risks and losses. Government provides for first responder and emergency management infrastructure to prevent hazards from becoming disasters and to lead the response and recovery from disasters when they do happen.

Public safety is a challenge for business and industry. Safety is a key element of sound business practice driven by ethical principles, the marketplace, government regulations, and liability laws.

Public safety is also the responsibility of citizens who are expected to take action not only to protect themselves and their loved ones, but also to make society safer through their community actions and their jobs.

Information is a cornerstone of public safety. We need to understand what the hazards are, when and where they occur, and how severe they are likely to be, before we decide to spend precious time and resources on mitigating them. Information may come in many forms and on many timescales. We receive warnings from product labels and manuals, from government regulations, and from the broadcast and print media. When time is of the essence, when action needs to be taken quickly, we use public warning to disseminate rapidly essential information to those who need it. Public warning, in this context, has the following characteristics:

The success of a warning is measured by the actions people take.

- A warning is a communication that directs attention to new information about a hazard or threat for the purpose of causing focused action that reduces harm.
- A warning may alert people to an imminent hazard or may notify them about a hazardous event that is in progress or just happened.
- A warning should communicate what, where, when, and how severe the hazard is, how likely the hazard is to occur, and what action is appropriate.
- A warning needs to communicate clearly and succinctly the risk people face, to motivate them to take specific action, and to provide guidance as to what that action should be.
- The success of a warning is measured by the actions people take.
- Public warning is a public good that is generally delivered through privately-owned communication networks and devices.

The roots of public warning are deep in American society. In 1776, Paul Revere warned that the Redcoats were coming. This timely warning empowered the Minutemen to prepare for and optimize their response to the hazard. With the advent of the commercial telegraph in 1845, advance warning of severe weather became practical. In 1870, President Grant signed a law requiring the United States Signal Service, part of the Department of War, to provide

weather warnings. Americans have also discovered the devastating effects of a lack of warning. In September 1900, a hurricane that was largely unanticipated killed at least 6,000 people in Galveston, Texas, the single worst loss of life from a natural disaster in U.S. history. On December 7, 1941, at Pearl Harbor and on September 11, 2001, in New York City and Washington, these lessons were horrifyingly reinforced. Today more than a dozen Federal agencies and many other government and industry groups, local emergency managers and first responders provide warnings not only for acts of war and severe weather, but also for accidents, health concerns, natural hazards, and acts of terrorism.

Technology is perhaps the easiest part of the solution. The challenge is to structure the available technological components beneath an umbrella of public/private sector cooperation and coordination and with policies and procedures in place to ensure rapid and effective operation of the system.

Our prized open society, our admiration for risk-taking, and the value we place on individual rights place us at greater risk from both natural and man-made hazards because we choose not to unduly constrain the actions of our citizens. This makes it even more important that when threats are anticipated that may affect the safety and security of our populace, we have the ability to advise those who need to know of the threat and to explain the actions that should be taken to protect life and property.

Recent events have demonstrated a clear need for improving the means and methods we utilize for collecting, analyzing and disseminating public warnings. Fortunately, advances in technology offer us an equally significant opportunity and flexibility to meet those needs. In fact, technology is perhaps the easiest part of the solution. The challenge is to structure the available technological components beneath an umbrella of public/private sector cooperation and coordination and with policies and procedures in place to ensure rapid and effective operation of the system.

Public Perceptions And Expectations

Over many decades, many of us have grown accustomed to hearing the following announcement:

> "This is a test of the Emergency Broadcast System. The broadcasters in your area have developed this system to keep you informed in the event of an emergency. If this had been an actual emergency, you would have received official instructions and information."

Most Americans believe that in a real emergency, they will be warned. They have become acclimated to this test message. They also instinctively compare emergency warning to their experience with the well-known methodologies employed successfully by the National Weather Service. Unfortunately, our national ability to provide people at risk with useful information to reduce loss during all types of emergencies is severely limited. With the increased likelihood of terrorism and the possible use of weapons of mass destruction, the potential for catastrophic loss of life is great. When poison gas is drifting rapidly downwind or a dirty nuclear bomb has contaminated a region, thousands of lives could be saved if

officials could quickly and effectively get the attention of people at risk and communicate how to get out of harm's way.

The public confidence that a nationally integrated warning system is already in place is amplified because many people already own devices that they believe could warn them. New warning devices are regularly being brought to market. Warning technology is evolving more rapidly than it can be effectively applied. The fundamental problem is that no entity has assembled the many different components into an integrated system. Rather, public warning exists as a collection of disparate components provided by many different organizations, at different times, and often with different design goals. The challenges are to integrate warning technologies into an effective, national, all-hazard capability for developing and disseminating warning messages, to institute the necessary policies and procedures for implementing and utilizing such a system, and to educate warning providers and the public.

The purpose of this document is to explain the shortcomings in our current national warning capability and to chart a course for providing warnings that address those shortcomings and better serve the needs of the American people.

Responsibilities

Government is responsible for the safety and security of its citizens.

The most basic responsibility of any government is to provide for the safety and security of its citizens. Government agencies at all levels have a collective responsibility to fulfill that responsibility.

With the well-established principles of federalism, states' rights, and local control, municipal, county, and tribal governments have the primary responsibility for public safety. They employ firemen, policemen, emergency managers, and others to provide this support. But disasters do not respect geographic or political boundaries. They often involve many localities. When disasters overwhelm both local and mutual aid resources, then regional and state government assistance is required. The Federal government plays a key role in responding to and recovering from any calamity that overwhelms the capabilities of state and local governments and that is declared a major disaster by the President (US Code Title 42, Section 5121, et seq.). The Federal government also plays an important role through its leadership in preparing for and mitigating potentially major disasters.

While some warnings originate locally (such as for accidents or criminal activity), others depend on synthesis of scientific or intelligence data at regional, national, and international levels. The facilities and resources needed to develop the many types of public warnings are greater than any one community can provide or even influence. That is why U.S. Code Title 42, Chapter 68, Subchapter II, Section 5132 states:

- The President shall insure that all appropriate Federal agencies are prepared to issue warnings of disasters to state and local officials.
- The President shall direct appropriate Federal agencies to provide technical assistance to state and local governments to insure that timely and effective disaster warning is provided.

- The President is authorized to utilize or to make available to Federal, state, and local agencies the facilities of the civil defense communications system … or any other Federal communications system for the purpose of providing warning to governmental authorities and the civilian population in areas endangered by disasters.
- The President is authorized to enter into agreements with the officers or agents of any private or commercial communications systems who volunteer the use of their systems on a reimbursable or nonreimbursable basis for the purpose of providing warning to governmental authorities and the civilian population endangered by disasters.

A fundamental goal of warning is to inform people at risk no matter where they are or what they are doing. This requires being able to issue warnings to people in very specific locations. Such targeted warning capability is a national challenge: it is too big to be addressed by individual municipalities, because it requires integration into products marketed nationally and the support of regional and national communications companies.

A national warning strategy is critical to effectively mitigate injury, death and damage to population and infrastructure. It is an essential tool needed by local emergency managers. It is also a key to implementing the national incident management capability set forth in the National Strategy for Homeland Security (www.whitehouse.gov/homeland/book/index.html).

A national strategy is required to ensure a single, common, integrated warning architecture for all municipalities.

A national strategy is also required to ensure a single, common, integrated warning architecture for all municipalities. Today many local communities have advanced warning capabilities; however, they are not interoperable with neighboring communities, agencies, other communications companies, or media. To reach people at risk in all locations and during all activities, we must have a common architecture that enables local government to perform its public-safety functions regardless of the origin of the warning or the nature of the emergency.

Those with leadership responsibility must now fulfill their public trust by integrating many diverse efforts into an effective and coordinated plan. Organizations, agencies and the public must work together to overcome the sociological/cultural, organizational, human, procedural and technological factors that currently stand in the way of implementing a nationally integrated and coordinated emergency warning system.

Stakeholders

When placed at risk, each of us has a stake in our public warning capability. At that moment, timely and accurate information can make the difference between life and death, between safety and significant loss. We, the public, are the primary users of public all-hazard warning systems, but there are many others who are stakeholders in public warning because of their direct responsibilities. For example:

- Federal, state, county, municipal and tribal governments all have responsibilities and critical roles in public warning.

- First responders, such as police, fire and emergency medical personnel, have a direct stake in public warning. Indeed, first responders are often the source of warnings (for example, if they discover hazardous material leakage when responding to an accident). A well-informed public does reduce the workload for first responders. Moreover, timely warning can enhance the first responders' situation awareness and can improve their leadership decisions and methods to mobilize limited resources. A national warning capability could be targeted at specific affinity groups to provide an effective alternative for mobilizing volunteer firefighters and recalling first responders when events suddenly turn life-threatening.
- Emergency managers in government and business are responsible for utilizing warning information and in many cases may also be the source of warning information.
- Scientists, intelligence experts, and many others develop warning information with the primary purpose of reducing losses. The value of their findings depends on how effectively they can communicate warning information to decision makers and to those at risk.
- Industry has the responsibility to research solutions, then implement and market quality technology in conjunction with services that leverage that technology. Industry can provide effective ways of integrating public warning delivery capability into our society and focusing those warnings on only those who need to know. The challenges facing industry must be addressed.

An Example of Successful Public-Service Collaboration

Where to recycle cans, bottles, or motor oil? What are the health conditions at a local beach? These are just a few of the environmental data that were dispensed by more than 10,000 websites and hotlines. Earth 911, a public/private partnership, now provides a single, bi-lingual portal to environmental information for all 50 states with participation by more than 3,300 counties and 10,000 localities (www.Earth911.org and 1-800-Cleanup). Now citizens can get the specific information they need by simply specifying their interest and their zip code. Local government did not have to pay for the system and now finds it much easier and less expensive to provide the information.

- Operators of critical infrastructure, lifelines, and transportation systems are all involved in warning systems.
- Insurance agencies have traditionally been proponents of warning since they have direct financial responsibility for the loss of life and property.
- The media play a major role in public warning and public education. Broadcasters and cable companies operate the national Emergency Alert System.
- Non-profit organizations such as the Red Cross play a major role in disaster response and public education and thus have a major interest in the effectiveness of warnings.
- Many volunteers assist in community safety issues and play a role in public warning and disaster preparedness and recovery.

- Many professional, trade, and advocacy groups represent first responder communities, the people who develop warnings, private industries, ethnic organizations and groups with disabilities.

All of the above have a direct stake in our national warning capability and have important roles to play in the specification and development of a national warning infrastructure. None, though, can individually address the challenges of "any time, any place" warning infrastructure. Only through an effective partnership of all the stakeholders, can the American people secure the improved national warning capability they deserve.

Cost Versus Benefit

Fortunately, the cost for government to implement a national, integrated public warning capability is measured in millions, not billions of dollars. All stakeholders need to shoulder the implementation, distribution, maintenance, management, support and service costs.

Industry needs a clear statement of government intent and clearly articulated standards that specify required interoperability for a national warning capability.

The Federal government cannot do it alone. For example, distributing a warning receiver to every citizen will not provide an effective national warning infrastructure. Experience tells us that people are unlikely to carry such a device at all times, and infrequent use would likely result in many receivers that are not in working condition when needed.

Many warning systems and devices that meet the needs of specific lifestyles and locations are available now, and new ones are being regularly introduced. Warnings are often not their primary function. Warnings to the public typically involve small amounts of information that can be fed into all types of wired and wireless data streams, and expressed or displayed through all types of appliances that may be routinely used for other purposes. The marketplace can drive the development and availability of such capabilities. But industry needs a clear statement of government intent and clearly articulated standards that specify required interoperability for a national warning capability. Industry will be naturally motivated to augment basic interoperability with competitive capabilities and refinements. The challenge is to develop effective cooperation and coordination between the public and private sectors.

A basic problem is to provide a coordinated means for collecting and inputting timely, standardized notifications into dissemination systems. Governments already provide major support in this area and simply integrating existing efforts can fuel more effective warning systems and offset data collection costs.

The benefits of implementing a national, integrated public warning capability are likely to rapidly outweigh the costs. There is ample evidence that warnings empower people to take actions that save lives, mitigate loss, reduce fear, and speed recovery. Besides the obvious savings in life and property, there are indirect benefits through reduced insurance costs and improved productivity -- not to say peace of mind.

There is a major need in America for a public warning capability that rapidly disseminates critically needed information to the widest possible audience within potentially affected groups. The technology exists to make a reliable national warning infrastructure. Lacking is a definition of the desired characteristics of the system, its standards, processes and the coordination of public and private efforts.

Current Public Warning Capability

Our current public warning capability consists of two national avenues for communicating among emergency managers and warning originators, two Federally led systems for communicating directly to the public, and a wide variety of warning systems designed, installed, and operated by private industry. Each of these systems meets specific needs, but their integration needs to be expanded to include all systems.

The National Warning System (NAWAS)

NAWAS is the primary national system for emergency communications among Federal, state, and local emergency operations centers (See FEMA Manual 1550.2, www.fema.gov/pdf/library/1550_2.pdf). FEMA operates two national warning centers: the FEMA Operations Center (FOC) at Mount Weather, Virginia, and the FEMA Alternate Operations Center (FAOC), in Thomasville, Georgia.

One New Approach To Emergency Communications

When disaster strikes our nation's capital, emergency managers in 18 local governments and numerous federal agencies need information quickly. The Metropolitan Washington Council of Governments, as part of their Regional Emergency Coordination Plan, installed in 2002 RICCS^{SM}, the Regional Incident Communication and Coordination System. RICCS^{SM} uses a commercially available universal communication platform that delivers text to any type of cell phone, pager or other wireless device to instantly alert all appropriate leaders and to convene conference calls to organize a regional response. This system is in daily use and proved extremely valuable during the sniper shootings in the fall of 2002.

NAWAS is a dedicated, 24-hour, specialized telephone line with 1,660 terminals that can be activated simultaneously but are more typically used in a hierarchical manner based on the region of concern. The FOC and FAOC can, with the push of a button, activate terminals for the whole nation, specific FEMA regions, or individual states using ten regional circuits accessing 300 terminals at primary and alternate state warning points typically located at the state emergency operations center and the state police dispatch center. The state warning points can then activate terminals at Local NAWAS primary warning points typically located at county emergency operations centers, law enforcement dispatch centers, or fire dispatch centers. State warning points are responsible for relaying most national information within their states and for relaying local information to other states when appropriate.

The District of Columbia and the National Capital area are served by the Washington D.C. Area Warning System (WAWAS), a separate circuit of 109 terminals managed by the Washington D.C. Office of Emergency Preparedness. This circuit can be manually bridged to the NAWAS regional circuit and connects emergency operation centers at surrounding key Federal agencies, airports, military installations, states and counties.

The FOC and FAOC also have direct links to the

Command Center at the North American Aerospace Defense Command (NORAD) and can relay appropriate information to the NAWAS circuits.

NAWAS was developed and installed during the Cold War to warn of an imminent enemy attack or an accidental missile launch upon the United States. It is now used primarily to disseminate warning information concerning natural and technological disasters and acts of terrorism. State or local government agencies qualify for a NAWAS connection based upon the eligibility criteria outlined in FEMA's NAWAS operations manual. These criteria take into consideration the size of the population served, proximity to another NAWAS connection, and the requesting agency's level of warning commitment.

Although NAWAS is a reliable system, there is some question as to its survivability. It is a system designed in the late 1950s, using 1950s telephone technology. In the 1990s, FEMA installed new terminal equipment at all NAWAS connection points that uses the same circuits that date back to the 1950s. The current monthly cost for operating NAWAS is in the area of $1.2 Million. Satellites might offer an alternate and perhaps more cost effective solution provided single point failure is taken into account and overall security is heightened.

Procedures for providing warning information through NAWAS for input to the Emergency Alert System and other dissemination systems also need to be reevaluated.

NOAA Weather Wire Service (NWWS)

A critical part of the mission of the National Weather Service (NWS) is the dissemination of severe weather warnings. NWWS is a satellite data collection and dissemination system operated by the NWS, whose broadcasts can be received anywhere in the United States and Puerto Rico. Its purpose is to provide state and Federal government, commercial users, and private citizens with timely delivery of meteorological, hydrological, climatological, and geophysical information from 141 NWS offices, the NOAA Space Weather Facility, and the U. S. Geological Survey's National Earthquake Information Center. NWWS delivers priority-warning products to users in less than 10 seconds. Warnings messages contain embedded digital information identifying the specific threat and area at risk. NWWS subscribers select the suite of products of interest to them.

NWWS can be received via C band and Ku band satellite receivers or over the Internet. NWWS downlinks are supplied to one emergency management agency in each state under an agreement requiring that they, in return, supply local hazard information to NWS for broadcast when appropriate. Access to NWWS is available to any qualified warning provider for warning delivery. Negotiations are currently in progress to interface the National Law Enforcement Telecommunications System (NLETS) with NWWS to allow an immediate interchange of all-hazard warnings with several thousand local law enforcement agencies around the country. There are currently 400 subscribers to NWWS, but they disseminate critical information to millions through radio, television, local emergency management networks and the private weather-forecasting industry. NWWS can activate the EAS or provide warning information for non-EAS broadcast. NWS is currently testing an internal quality control mechanism for NWWS that will add an email warning delivery capability.

Emergency Alert System (EAS)

The EAS is our primary national system for warning citizens directly. The change from the Emergency Broadcast System (EBS) to the EAS occurred on January 1, 1997. The EAS serves two functions:

- Provide the President with the capability to deliver immediate communications and information to the general public at the National, state and local area levels during periods of national emergency.
- When not being used by the President, provide the heads of state and local government, or their designated representatives, with a means of emergency communications with the public in their state or local area.

The EAS operates under regulations specified by the Federal Communications Commission (FCC) (47 CFR Part 11, www.fcc.gov/eb/eas/rules.htm). Essentially, all 14,000+ radio and television broadcast stations and 10,000+ cable systems in the United States are required to install and test EAS equipment and rebroadcast a Presidential message that could contain warning or emergency information. Any station that does not participate is mandated to go off the air for the duration of the message. At the state and local levels, EAS is a voluntary, cooperative effort and operates as an unfunded Federal government mandate, relying almost totally on the volunteer efforts of industry as well as state and local officials. Federal funding is minimal, and outreach and training efforts have steadily decreased since 1995. While there is no official EAS accounting system, only 50 to 60% of the broadcast stations appear to relay state and local emergency messages.

The EAS reaches a limited number of people. Radio stations reach 95% of Americans older than 12, but Americans listen to the radio on average only 12% of their day, mainly between 6 a.m. and 6 p.m. (Arbitron, 2001 Radio Today). While as much as 22% of the population may be listening at any given time during the day, less than 1% are listening in the middle of the night. More than 98% of U.S. households have at least one television but the average set is in use only 31% of the day (Nielsen Media Research, 2000 Report on Television), and 17% of households (Satellite Broadcasting and Communications Association) now get their signals directly from direct broadcast satellite sources that do not participate in EAS. While the EAS does include codes that could activate devices while people are sleeping or otherwise not tuned in, only a few companies are producing such devices.

The EBS was originally a joint venture. In 1981, the FCC, NOAA (which includes the NWS), the Defense Civil Preparedness Agency (now a part of FEMA) and the FAA's National Industry Advisory Committee updated their Memorandum of Understanding (originally signed in 1976) to develop detailed state and local plans to use EBS for state or local emergencies. Until this time, state or local authorities rarely used EBS for natural or man-made disasters. The federal agencies provided on-site assistance in the states and territories to broadcasters and state and local officials in their EBS planning. Also, a "Plan for Nationwide Use of the Emergency Broadcast System for State and Local Emergencies" was developed as a guide to implement the agreement.

This coordinated effort resulted in the development of state plans throughout the U.S., including more than 400 local areas. When EAS was established in 1994, there was a need to update the EBS plans. The great majority of the planning work fell to industry, and to state and local government volunteers. The fact that EAS works at all at the state and local level is directly traceable to this volunteer effort. However, 11 states and territories still do not have final EAS plans and only 100+ local plans have been finalized (www.fcc.gov/eb/eas/plans.html).

No President has ever chosen to utilize EAS or the EBS before it, even though procedures and protocols exist for immediate Presidential access at any time or place. The voluntary nature of EAS at the state and local levels has limited its effectiveness primarily through lack of adequate planning.

Other significant limitations of EAS include:

- EAS currently can only be focused on people at risk by county, but broadcast stations typically reach many counties. Thus, EAS in many cases may warn large numbers of people not at risk. Additional codes to specify 1/9th portions of counties are available, but are not in common use.
- The EAS national distribution system for Presidential messages, the Primary Entry Point system (PEP), utilizes 34 major broadcast stations and one broadcast network. It does not currently reach all state EAS entry points and it uses standard telephone circuits as the main communications link from the Federal government to the PEP stations. Regular tests conducted by the FOC and FAOC often do not trigger and successfully test all 34 stations.
- Successful state and local EAS operation depends on development of state and local plans that specify which messages will be sent, who can originate messages, how originators and broadcast and cable systems are linked, and regular testing procedures. Many regions do not have such plans.
- EAS alerts, warnings and other messages are sent using specific digital codes that control operation of the EAS equipment. In 2002, the FCC agreed to add several important codes, including one for Amber child abduction alerts. EAS equipment must be upgraded to respond properly to these new codes, but the FCC did not make upgrades of equipment already installed mandatory.
- The FCC's EAS National Advisory Committee (NAC) charter was not renewed in mid 2002, causing a loss of a key communication and coordination resource for state EAS Chairs and other EAS stakeholder volunteers.

Warning Confusion

The Homeland Security Advisory System (HSAS) is regularly in the news. People are confused about what the colors mean and what they should do. The HSAS is not a warning system. It does not provide enough specific information to allow decision makers to make rational decisions about spending precious resources to prepare. HSAS is essentially a "hot tip" based on non-specific intelligence information. As such, it can encourage increased vigilance and awareness for short periods of time. Problems with HSAS illustrate the difficulties in communicating risk effectively.

- Presently, more than 80% of EAS messages are weather-related and generated through monitoring NOAA Weather Radio. Few EAS messages are generated by state and local emergency managers, partly because few have the equipment to input warnings directly.
- EAS transmissions are not secure from hacking.
- EAS communications protocols and equipment are limited in their capacity and capability to handle further development of the system.
- To date, the FCC has not incorporated EAS into High Definition Television, satellite-delivered television and radio, or digital radio. These technologies offer important new possibilities and will be attracting an increasing percentage of the listening and viewing audience.
- Expansion of the use of EAS would be of more interest to broadcasters and advertisers if it did not interrupt programming for those not directly at risk.

NOAA Weather Radio (NWR)

The other primary national method for delivering warning messages to the public is NWR, an audio broadcast of weather information and warnings. The signals are accessible to 95% of the American population in fifty states, Puerto Rico, the Virgin Islands, Guam, and the Mariana Islands. More than 770 NWR stations broadcast locally specific programs from 120 NWS Offices. Warnings have embedded digital information that identify the specific threat and area at risk. This coded information, identical to EAS coded information, can trigger alarms on low-cost programmable receivers that allow listeners to select the locale and warning events that are important to them. NWR and EAS messages can be sent to specific geographic regions dictated by distance from the transmitter and specified by codes for specific counties. Additional codes to specify $1/9^{th}$ portions of counties are available, but are not in general use.

Many brands and types of NWR receivers are available. Some are now being built into car radios, televisions, and other general use devices. The receivers provide warning access to the deaf and hard-of-hearing community. A recent national survey of 1,000 people concluded that depending on region of the country from 8% to13% of U.S. households have NWR receivers (eBrain.Consumer Research for the Consumer Electronics Association, 2002). Every commercial radio, television, and cable TV station is required by the FCC to have EAS equipment installed that includes a built-in NWR receiver programmable to automatically and immediately rebroadcast NWR warnings as an EAS activation. The warnings received over NWR may also be used at the discretion of broadcasters as non-EAS broadcasts. Many state and local governments have provided NWR receivers to schools and hospitals. NWR stations are also used by a number of biological and chemical weapons storage areas and nuclear facilities as their mandated warning systems. NWR was recently sanctioned by FEMA for delivery of all-hazard warnings. NWR stations are now available for dissemination of all hazard warnings by national, state and local emergency management agencies. While a growing number of these agencies provide civil warnings to NWR, most still do not.

Needed improvements and enhancements are being mapped out. Internal NWS networks now loosely couple NWR and NWWS. NWS is exploring an integration of NWR and NWWS that will significantly improve the quality and reliability of warning delivery and create a more robust network architecture. Combined with planned efforts for a more secure electronic interface, an integrated NWR/NWWS should allow immediate access to any transmitter or group of transmitters in the NWR and the NWWS network by any approved warning source (local, state or national) for all-hazard warning dissemination to those at risk at any time.

There are more challenges. While the infrastructure for NWR is a significant national asset, as noted above only from 8% to 13% of the population actually owns the special receiver and only half of those receivers are portable. Few people carry these receivers with them every day. The principle shortcoming of NWR in broadcasting terminology is listener market penetration. NWR, like EAS, is also limited in its ability to target people at risk only at the county level and in some cases the 1/9th county level.

Other Warning Systems

A wide variety of warning systems are designed, installed, and operated by private industry. Receivers may be specialized equipment or commonly available devices such as telephones or computers. Many of these systems are present around critical locations such as nuclear facilities, chemical stockpiles, oil refineries, and dams. Many states and municipalities have installed them. The principal limitations are that they are usually not interoperable, do not typically have all-hazard inputs, and their availability varies widely across the country.

Today, many companies provide warnings on a subscription basis through computerized calling systems, fax, email, or digital messaging to all types of devices. After 9/11, Congress bought such a system for its own use. Those who can pay and are willing to share personal contact information with a company can receive a variety of warnings via currently available technology. However, none of these companies have access to a complete and reliable stream of all-hazard warnings for most areas.

New methods and devices have been developed to improve warning delivery, but many of the companies behind these systems are facing insurmountable obstacles to implementing their technology. Significant issues include:

- Lack of participation by carriers and broadcasters.
- Impact of mixed messages from the Federal government regarding national systems in place and what might become of them.

Building Warning Capability Into Consumer Electronic Devices

January, 2003, Microsoft announced with several watch manufacturers a new national service that can deliver critical information such as warnings to wrist watches.

February, 2003, Thomson announced AlertGuard^{TM}, a warning capability that will be built into many of their RCA brand television sets. The televisions will include a NOAA Weather Radio receiver. Users will be able to determine how they wish to receive warnings including waking the user in the middle of the night if he or she is directly at risk.

Many other companies are exploring ways to add warning capability to their consumer devices.

- Lack of an infrastructure to provide the hazard information.
- Availability of quality data required to support such methods.

As a result, these companies are finding it difficult to attract venture capital to support their efforts and to retain the interests of large communications equipment and system providers, many of whom were involved in public warning and have since left the industry.

Problems With Current Warning Systems

The basic problems with current public warning systems are as follows:

- Warnings do not reach enough of the people at risk and often reach many people not at risk.
- Most warnings cannot be issued to just the people at risk except by calling wired telephones using the 911 database. The EAS and NWR can only specify which county and sometimes which 1/9th of a county is at risk.
- Few local emergency managers or first responders have effective ways to input information and warnings into these systems.
- Warnings from different sources are rarely available to all warning systems in a given region.
- There are few standards, protocols, or procedures for developing and issuing warnings.
- Warnings from different sources use different terminology to express the same issues of risk and recommended action.
- Many systems are not interoperable.
- Even the national Emergency Alert System has increasing points of potential failure due to decreased funding and a lack of action in developing state and local plans for proper utilization.
- There are no metrics for measuring the effectiveness of current warning systems.

Many dedicated people are maintaining existing systems, often on a volunteer basis, but this patchwork quilt is nowhere near as effective as it could or should be.

Many dedicated people are maintaining existing systems, often on a volunteer basis, but this patchwork quilt is nowhere near as effective as it could or should be.

Improving Public Warning Capability

The goal of a public warning capability is to reach virtually every citizen at imminent risk from natural or manmade disasters in a timely manner, no matter where they are or what they are doing, in order to provide critical information that will empower them to take actions to reduce loss. Such a system is more complicated than many appreciate. Here are some of the basic issues.

Ethical Values

A national warning capability should be founded on a code of ethics based on moral values common to all humanity and on fundamental principles of American culture.

Value of life: Investing time, effort and money to protect and save lives is ethically and morally justified. The investment is also economically rooted, justified by the value of a person's work and contribution to society. Warning development, conveyance and reception should not place the lives of those who warn or those who are warned at additional risk.

Obligation to warn: Individuals, businesses, communities, organizations and governmental agencies that create, generate or hold information that can reduce risk have a fundamental moral duty to warn of impending danger.

Freedom of choice: People have the right to make decisions that affect their lives and property and they should have access to information required to make sound decisions.

Respect for privacy: Warning systems need to respect individual privacy both in the use of personal information and in how people are notified.

Ingredients of a Successful Warning

On November 11, 2002, a tornado destroyed major parts of the Van Wert Cinemas in Van Wert, Ohio. The National Weather Service had issued a tornado alert that was received over NOAA Weather Radio at the county emergency operation center. The county relayed the alert to movie theaters, shopping centers and other populous locations using a system they had installed just two years before. The theater manager already had a plan in place that called for moving patrons into corridors and restrooms that were more resistant to tornadoes. He moved 50 people to safety moments before the roofs were torn off two theaters and several automobiles were dropped from the sky onto seats where children had just been sitting.

Basic Principles

Warning delivery capability must be ubiquitous: This can be done most efficiently by adding the warning feature to devices in wide use for other purposes.

No single methodology will meet all needs: Research shows clearly that more than one channel of communication will be consulted by people at risk in order to confirm the need for action. Each methodology has its benefits and drawbacks.

Government should support private sector development by providing clear direction and not competing with those processes.

No capability is perfect: The stakeholders and the public need to understand and acknowledge that the risk of untimely or incomplete warning can not be completely eliminated but can, and must, be reduced.

Preference for market solutions: Our society relies upon the free market to provide optimum solutions. While governmental leadership is required, any delivery solution should be based upon marketplace mechanisms. Government should support private sector development by providing clear direction and not competing with those processes.

Of clear value to all stakeholders: A national warning capability must provide clear value to all stakeholders so that they can work together enthusiastically to improve dissemination and assimilation of this real-time information.

Functional Values

A national warning capability should be:

- **Focused**: Warnings need to be focused on the people at risk, the first responders, and others with a need or desire to know while respecting their privacy. Warning people not at risk will degrade confidence in the system and may make it more difficult for people at risk to take appropriate actions.
- **Available:** The system must reach people no matter where they are or what they are doing. The system must reach people whether they are awake or asleep. The warning receiver should be immediately available and not require any specific action to enable it during a threat.
- **Accessible:** The system should be designed for use by handicapped individuals, including those with hearing, sight, mobility, or literacy limitations . Access for the elderly and children is imperative. Where feasible, the system should allow for different languages.
- **Safe**: Message delivery should not inadvertently add risk to those providing or receiving the warning.
- **Easy to use:** The system should not require detailed training or programming in order to be understood or utilized. Interfaces for the public should be intuitive and extremely simple to use. A variety of interfaces will allow recipients to choose one that suits them. For first responders, the interface should be integrated with their other communications devices so that it is a familiar part of their tools.
- **Reliable**: The methods of message generation, transmission, and receipt must be reliable or citizens and emergency personnel will not use the system.
- **Timely**: Effective warnings must reach the people at risk in as timely a manner as possible.

- **Secure**: Access to warning systems and the authority to initiate a warning must be restricted to appropriate personnel or organizations so that warning recipients can trust that the warnings they receive are authentic. On the other hand, excessive security provisions can cripple the ability to efficiently disseminate information.
- **Widely Recognized**: Need to ensure that the warning network is a household name and the public is aware of and empowered with its functionality.

Warning messages need to be:

- **Accurate**: Inaccurate warnings will undermine credibility in the system.
- **Understandable**: The nature of the threat must be easily identified to the citizen. Sufficient information must be included to allow informed response to threats and to serve as the primary "24/7" notification source. The use of common terminology across different hazards will make warnings easier to understand.
- **Specific:** Providing focused, scalable information to each user is important. Decision makers will require detailed information. Other users may need only enough to inspire action, which is spurred by multiple corroborating sources that convey the same specific information.
- **Action oriented**: Suggesting appropriate actions helps users protect themselves from a threat and increases the effectiveness of warnings.
- **Locally Controlled**: Locally authorized individuals need to have ownership and control of their information to ensure buy-in, accuracy and confidence of the affected public.

Warning Process Elements

A system to deliver effective warnings has many critical elements from original data to action.

A system to deliver effective warnings has many critical elements from original data to action. To make the process more effective, each element must be reviewed and optimized so that warnings can be developed and delivered with maximum accuracy and with minimum time and committed resources. A fundamental concept to optimize the process is to never lose sight of the individual or group that is receiving the benefits of each element. The ultimate customer for the total warning capability is the public. At different steps in the process, customers include emergency management organizations, warning dissemination providers, forecasters, etc. The needs of the customer and supplier must be provided for in each step of the process. Here is a summary of the important elements of a process for developing and delivering public warning messages:

- **Data collection, analysis, and decision making**: Development of evidence of a hazard through collection of data and information, their analysis, and the process by which a decision is made to issue a warning.
- **Framing a warning**: Specifying a verbal and digitally coded warning message using standards for terminology and format based on knowledge of how to trigger an

appropriate response. The nature of the threat must be readily identified to the user. Sufficient information must be included so as to allow informed response to threats regardless of time or location.

- **Reliable warning input**: Assure secure collection of warnings from thousands of authorized sources into local and national communication avenues that can deliver the warnings to a wide variety of distribution systems.

Taking Action

Social scientists find we commonly take several steps in deciding to take action:

1. Perceiving the warning (hear, see, feel)
2. Understanding the warning
3. Believing that the warning is real and that the contents are accurate
4. Confirming the warning from other sources or people
5. Personalizing the warning
6. Deciding on a course of action
7. Acting on that decision

- **Transmission to warning distribution systems**: Redundant and robust transmission along local and national avenues for input to a wide variety of distribution systems.
- **Transmission to end-user devices**: These may include local mass warning devices (such as sirens or public address systems) and intelligent networks/receivers that notify people based on their location or interests. Ability to direct the message to a specific geographic area (or demographic community) makes the message more useful and increases warning accuracy.
- **Warning Announcement**: Announcement of the warnings in an appropriate language and process by activating devices that can deliver the warning to people who need it no matter what they are doing or what physical or mental limitations they may have.
- **Decision to take appropriate action:** The process by which the end-user decides to take action and indeed takes that action, which might include warning others.
- **Requirement for further action:** Analysis of how effective protective actions have been and how the threats have been evolving over time. Issuance of additional warning as appropriate.

In addition, many continuing processes are required to improve the effectiveness of warnings:

- **Planning**: Related to all aspects of framing, delivering and utilizing public warnings.
- **Education:** Inform and instruct decision makers, the media, and the public on warning terminology and response.
- **Ongoing evaluation**: Conduct periodic and after-action audits to verify that systems and procedures are functioning as intended and have not been misused. Create and implement a system for evaluating effectiveness, testing operational components, and introducing improvements.

Challenges

Interoperability

A fundamental problem today is the lack of technical and procedural interoperability among warning originators, system providers, warning recipients, and delivery systems.

Originators must now undertake redundant tasks using multiple, dissimilar tools and techniques to take full advantage of the warning capabilities available to them. And the creation of "ad hoc" warning capabilities in response to unusual situations is slowed and complicated by the lack of interoperability among existing warning systems.

Providers of warning systems are denied the economies and efficiencies of scale that can be achieved when their products, and related products, can be interconnected without special effort. Additional costs of customizing "one-off" system interfaces reduce the attractiveness of investment in warning systems. And the absence of an interoperability strategy for warning systems increases uncertainty regarding technical and procedural designs.

A fundamental problem today is the lack of technical and procedural interoperability among warning originators, system providers, warning recipients and delivery systems.

There is also a major need for an interoperable backbone capability for exchanging and coordinating warning messages. Many emergencies lead to the issuance of warnings from multiple sources. For example, a major event in a metropolitan area may activate warning functions in dozens of jurisdictions and hundreds of agencies. Requiring all warnings to be issued from a single center can create an information bottleneck; even when this does not result in delays or failures, it may lead to loss or distortion of location-specific details. This in turn can lead local officials to feel they have no choice but to issue their own warnings anyway. The resulting chaos can reduce warning effectiveness and damage the credibility of warning sources and channels.

Interoperability is also required for delivery systems to increase technical reliability. Each technology has weaknesses and vulnerabilities, so a mixture of technical systems reduces the risk of common-mode failure.

A single warning is frequently insufficient to move people to action, especially if it cannot be confirmed by direct observation. For most people the first warning received captures their attention and triggers a search for corroboration, but cannot be relied on to elicit the desired behavior. Scientific research supports the common-sense observation that people are disinclined to risk being fooled by a single alarm that might prove false or accidental. Effective warning requires the coordinated use of multiple channels of communication. Again, the lack of interoperable warning systems and an integrating framework raises a barrier to warning effectiveness.

Nor is interoperability just a technical problem. There is no generally accepted vocabulary for expressing the nature or severity of a threat, the immediacy or urgency of a warning, or the

degree of certainty of the warning information. Different language used by different authorities can cause confusion for the recipients even though the actions required are limited and common among most hazards.

Leadership

Within government generally, and particularly at the Federal level, there is no overall "owner" who is responsible for the public warning function. As a result, responsibility for the development and use of warning capabilities is fragmented among many agencies and jurisdictions, with little or no means for coordination. In particular, responsibility for developing warning facilities, procedures and resources is frequently separated from the responsibility for actually using them.

There is no overall "owner" who is responsible for the public warning function.

Facilities and procedures for threat detection, decision-making and message dissemination are being created by government and non-government organizations with regard only for their particular responsibilities. In the absence of unifying leadership, the differences in priorities and scope among organizations with warning responsibilities, combined with their inherent desire for operational autonomy, frequently lead to miscommunication and even mistrust that can delay or derail worthwhile collaborative efforts. This problem becomes particularly acute in systems that involve both public and private sector components, such as the EAS.

In addition, with no agency with overall responsibility it is extremely difficult to identify, obtain and apply funds to correct a wide spectrum of warning infrastructure problems. Investments in warning capabilities are made piecemeal, without common evaluation criteria or requirements. In the process, potential economies of scale are lost, best practices are not shared, and new systems are created that cannot communicate with each other.

More fundamentally, there is no one to articulate and codify the principles that should guide warning processes. A number of agencies and organizations have specific policy or regulatory guidelines regarding when and who to warn, what the form of the warning should be and how it should be delivered. However, there is no clear set of principles or standards of practice to aid decision-makers during novel, unforeseen circumstances.

The decision to issue a warning often involves weighing a complex mix of factors, including the urgency, severity and certainty of the threat, the level of confidence in the available information, and (unfortunately) the potential financial, political and personal costs of error. Knowing that any warning decision may be criticized, and without any standard against which to measure a situation (or to explain or defend a choice), warning decision-makers are placed in a no-win situation. As a result, warning decisions are often delayed or never issued.

Security

Access to warning systems and the authority to initiate a warning must be restricted to appropriate personnel or organizations. In addition, warning recipients need to be able to trust that the warnings they receive are authentic. On the other hand, excessive security provisions can cripple the ability to efficiently disseminate information. An overblown fear of inciting public panic (which is, in fact, extremely rare) can lead to a paralyzing fixation on security over all other considerations. Security is never an absolute; real-world security planning involves balancing risks against the benefits of timely and efficient task performance.

The lack of systematic evaluation and audit can make warning-system security a matter of speculation rather than knowledge. Independent auditing processes and performance measurements are required, which entails providing appropriate independent access to system performance data. Both periodic and after-action audits are needed to verify that systems and procedures are functioning as intended and have not been misused. At the same time, careful attention must be paid to ensuring the protection of personal and proprietary information.

Legalities

Many legal ramifications of warning practice are unclear. In many cases it is unclear whether any affirmative "duty to warn" exists, and if so, where it lies and what its limits may be. We have no professional standard of warning practice, and many of the programmatic and regulatory requirements that do exist are narrowly drawn and dispersed across many agencies and levels of government and the private sector. As a result, the technical capacity of warning systems can be rendered moot by operators' uncertainty about what decision-making principles should apply.

Government should not mandate solutions without considering the impact upon other stakeholders.

Various other issues of privacy and freedom of information arise in governmental warning processes. When private industry plays a major role, other issues arise over intellectual property such as database access. Liability questions are endemic. The limited bodies of explicit legislation and clearly applicable case law are insufficient to relieve uncertainties that can inhibit both development and use of warning capabilities.

Business Concerns

In the absence of a coherent national warning strategy, companies have become hesitant to expend development funds on new warning products, and investors have become wary of the warning industry. In the last few years, many of the largest communications companies have reduced or eliminated their investment in public warning, at a time when the need has never been clearer or greater. Sales and new product creation are inhibited by uncertainty about future national policies and standards, as local governments wait for state and Federal governments to tackle the issues that must be addressed before they can implement truly effective solutions.

This leaves owners and operators of existing warning systems with the unhappy choice of continuing to invest in increasingly incomplete and sometimes obsolete products or of simply taking a “wait and see” stance, not maintaining, expanding, or even implementing warning capabilities. This inhibited market further reduces the incentives for product enhancement and development, completing a vicious circle that leaves the nation with an increasingly obsolete and unworkable warning infrastructure.

Government leadership should not mean unfunded government mandate. Many companies have avoided public warning out of fear of government mandates. There are two clear examples. Broadcasters, as a condition of their licenses, operate the Emergency Alert System while the FCC can and does mete out fines for non-compliance. The need to locate cellular telephones when they are used to call 911 is also now mandated on the telecommunication industry. In both cases, unfunded government mandates have not typically led to the most effective solutions. Public warning may require some level of government-enforced standardization and a minimum standard of service, but such decisions need to be based on consensus of the many different stakeholders and the acceptance of most organizations affected. Through an effective public/private partnership, government can keep the control it needs while bringing out enthusiastic participation of others.

The Need For A Backbone

Industry is developing a wide variety of ways to deliver warnings (Appendix 3), but there is no place to “plug in” to receive all warnings for a given region. A backbone would collect warnings from thousands of reliable sources, in secure ways, using standard terminology and protocols and make them available locally and possibly even nationally to warning delivery systems. A backbone may also assist in the considerable communication required between scientists, intelligence experts, emergency managers, first responders, health officials, critical facilities managers, and many others when warnings are being developed and issued. Such a backbone should leverage existing and developing public and private networking capabilities. Much could be done on the Internet with appropriate backup channels to assure reliability and speed during times of crisis. The stakeholders need to define the specific needs and to explore the options.

Plan for Action

Processes Required

In order to develop a unified public warning capability that will meet the needs of the American people for natural and man-made hazards, we believe that the Federal government must lead a nationally coordinated effort that will equally involve municipal, county, state, and tribal governments as well as stakeholders in private industry and other organizations, including volunteers. For this warning capability to be a success, one single Federal agency needs to be responsible for ensuring that national systems and procedures exist, are effective, and are properly utilized to distribute warnings and information for all types of hazards to and from all stakeholders and ultimately to those at risk. Under the leadership of this agency, all stakeholders must work together to develop:

- A clear statement by government of national needs, expectations and a timeline.
- A diverse Public Private partnership that can coordinate and manage the intricacies of the network without the limitations, both time and money, caused by a fully government controlled program.
- A clear understanding of stakeholder roles.
- Professional standards for how warnings are developed and disseminated.
- A unified, all-hazard terminology for communicating risk and appropriate action.
- A standard message protocol that will allow interoperability among all types of warning delivery systems.
- Procedures for inputting warnings into dissemination systems.
- Procedures to facilitate message-targeting decisions during a crisis.
- Methods for distributing warnings from throughout the nation into delivery systems.
- Plans for training, exercising, testing, and improving warning capabilities and procedures.
- A capability for industry to assess market potential and thereby develop creative and competitive ways to meet these national needs.
- An understanding by all people at risk and emergency responders of the criticality of a national system and the importance of planning and preparing for response to disasters.
- An optimization of the process for speed, reliability and accuracy.

The development of these standards and procedures will allow the individual stakeholders to develop component systems for the warning process within the framework of a national warning capability. The standards developed will support the efficient, reliable, and successful operation of this capability. Without them, it will be difficult for the stakeholders to work together or for venture capital to be raised to finance new systems.

This would seriously delay improvements to our current warning capability. With them, the development process will have many built-in incentives for success.

Practical Possibilities

If we act now, every American at imminent risk can soon have:

- Immediate and unrestricted access to public warning.
- Choice of the method of information delivery.
- Knowledge of how to take appropriate action.
- Follow-up information and education during and after the event.

The first steps are to:

- Decide that improved warning capability is a national priority.
- Designate a senior Federal officer responsible for overseeing significant improvement of public warning capability.
- Institute processes that bring representatives of all stakeholders together to develop standards and procedures for a public warning capability.
- Appropriate modest funding to enable this work.
- Assess in detail current warning capability for the first time.

Within two years:

- Develop a standard, all-hazard terminology for warning.
- Develop and test a prototype standard protocol for warning messages that will enhance interoperability.
- Develop criteria, prototype and test a design for national warning avenues/backbones to collect warnings from all appropriate sources and provide them as input to appropriate dissemination systems.
- Create professional standards for developing and releasing warnings, including planning for the makeup and operation of decision-making teams for a wide variety of hazards.
- Implement an active research program focused on public warning effectiveness.
- Develop an ongoing forum that includes technical experts, emergency managers and responders, and social scientists in order to implement the results of this research.
- Develop metrics for measuring public warning effectiveness.
- Improve access to emergency response databases.

- Begin training and exercising local, state, and national groups responsible for public warnings.
- Begin public education on warning issues.
- Encourage a significant infusion of capital into the public warning industry.

Within five years it should be possible, if adequate funding continues, to:

- Fully implement the standard terminology and protocol.
- Complete professional standards and the national warning backbone.
- Complete public rule making.
- Implement many of the research findings.
- Adequately train and exercise groups responsible for warnings.
- Make public warning information readily available as a small part of widely distributed documents such as telephone books.
- Have a healthy public warning supplier industry, with participation by many of the country's largest communications companies.

With this strong foundation, industry can begin to integrate warning capability into a wide variety of devices used daily for other purposes. Such integration would mean that Americans could go about their daily lives without concern for keeping warning channels open. However, in those rare circumstances when they are directly at risk, public warning information would be readily available no matter where they are or what they are doing.

Committing to such a process and goals would have an immediate effect on improving warning delivery capabilities by empowering the stakeholders:

- Industry would understand that this is a national priority, would participate in developing and adopting standards that they can depend on for making business decisions, and would appreciate that there is market potential in integrating warning capability into their products and services.
- Current providers would begin working together to standardize their warnings and aggregate them into national backbones to which industry could connect.
- Current providers of warning delivery services would get better access to all types of warning information.
- Municipal, county, and tribal governments could begin realistic planning for providing warnings to their citizens.
- The public would understand that improvements in warning capability are being implemented and would begin learning more about how they should be prepared to respond to warnings.

Required Stakeholder Actions

The Federal government must provide leadership and funding for developing a national public warning capability, but it cannot and should not solve this problem alone. The fundamental challenge is to find ways to weave warning capability into the very fabric of our society; ways that are effective and respect individual rights. This effort will take teamwork and partnership that will not only unleash American ingenuity and entrepreneurial skills, but also reduce the costs through improved efficiency and sharing. Consumers will pay much of the cost through very small increases in price for products they normally use or through the desire to buy more specialized devices or services. The economies of scale provide remarkable incentive when you want to reach all citizens one way or another.

There are numerous stakeholders of public warning systems and they all need to play significant roles to meet the national need.

The President and Congress should:

- Make an integrated public warning capability a priority for the nation.
- Assign lead responsibility to the Secretary, Department of Homeland Security.
- Establish a process by which all national stakeholders can participate effectively in the development of this national capability.
- Provide appropriate Federal funding for integrating public warning policy and capability.
- Fund research and operational capability for information gathering systems that will make warnings more reliable.

The Secretary, Department of Homeland Security should:

- Delegate the primary operational responsibility to a senior officer of the department with a staff to coordinate among Federal agencies and to enable an effective process that involves the stakeholders.
- Establish an inter-agency coordination board that brings key Federal agencies together to oversee details of the program.
- Provide policy, regulatory, and budgetary oversight over all Federal stakeholders.
- Set up and utilize processes that involve representatives of all the stakeholders in critical decision making and standards development.
- Assure meaningful involvement of Federal, state, county, municipal, and tribal authorities.

Other Federal stakeholder agencies should:

- Establish a primary point of contact for coordination with the Department of Homeland Security and with processes involving stakeholders.

- Reassess their responsibilities and roles in public warning and explore ways to consolidate and integrate these into a national effort.
- Reevaluate regulatory responsibilities to reduce the risks and create opportunities for companies to improve the national public warning capability.

State, county, municipal, and tribal governments should:

- Reassess the hazards they face and their needs for utilizing a national warning capability.
- Become involved with other stakeholders in representing these needs.

Private industry should:

- Participate actively in development of standards.
- Explore options for integrating warning capability into their products and services.
- Evaluate the role of warning in their business reliability and continuity plans and address these needs.

Non-profit, professional, and trade organizations should:

- Represent their interests in stakeholder processes.

The media should:

- Educate the public on the importance of a national warning capability.
- Establish partnerships with other warning stakeholders to enhance operational cooperation and communication.
- Encourage debate and citizen involvement in working with other stakeholders to develop this capability.

The general public should:

- Express to their representatives the need to improve warning capabilities.
- Represent their needs and concerns in partnership activities.
- Learn about and plan for appropriate responses to warnings.

Required Collective Actions

Principal actions for all stakeholders to move toward a national public warning capability include the following:

- Assess current warning capabilities and produce an analysis of what is needed to reach our vision.
- Develop a common, standard, all-hazard terminology for warning.
- Develop a standard protocol for warning messages.

- Develop metrics for measuring the changes in and success of public warning systems.
- Develop standards of professional practice for developing and issuing warnings.
- Develop standard procedures for public warning.
- Develop national backbones for securely and reliably collecting warnings from all appropriate sources and making them available to a wide variety of dissemination systems.
- Develop pilot projects to test concepts and approaches for improved public warning.
- Carry out research on ways to make public warning more effective.
- Develop education and training programs for people involved in the warning process and for the citizens at risk.

Funding Options

The Federal government has the responsibility to initiate development of a national, integrated, public warning capability. Any Federal investment, if spent wisely, is highly likely to foster similar funding in cash and in kind from other sources.

Federal funding is needed to establish processes that bring representatives of all the stakeholders together as equal partners on issues related to developing a national warning capability. For the first two years, these groups will need funding to:

- Develop benchmarks for assessing current warning capabilities and conduct objective assessments of existing capabilities.
- Conduct research on the current awareness of and effectiveness of existing national warning capabilities. Audiences for the research would include emergency managers, government officials and the public.
- Develop and recommend standards and guidelines for all-hazard terminology, common message protocols, warning processes and procedures and other key issues.
- Develop specifications for a national backbone to be used for collecting warnings from designated authorities and routing them to appropriate dissemination systems.
- Conduct pilot projects on warning processes, procedures and technologies.

Beyond year two, emphasis will need to be placed on:

- Implementation of national standards and the national backbone.
- Training and testing the national capability.
- Public education

What will it cost to implement this national public warning capability? And when will American taxpayers realize a return on their investment? While this is a national strategy paper, it was considered prudent to include an initial estimate of what is required to bring it to fruition. An important advantage of this plan is that most of the government's costs are up front … to prime the pump. The amount invested depends on how quickly you want to see the results. An initial outlay could be as little as $5 million annually, but progress will be slow. On the other hand, an investment of no more than $15 million per year over the next two years would allow implementation of significantly improved national public warning system. Once that happens, it is not anticipated that large amounts of Federal funding above current levels will be either required or appropriate.

Moving Forward

We all have a shared duty and obligation to act. September 11th taught us that the unthinkable is no longer an excuse for delay. Future tragedies are not a matter of if, but when. Lives can be saved and losses reduced through effective public warning. Americans expect their government to protect them and believe an effective warning capability exists. However, an effective warning capability does not exist, and it is only as matter of time before our nation will come to wish it did.

An effective warning capability not only can exist … it must exist. The time to act is now.

Appendix 1: Report Writing Committee And Reviewers

The following individuals initially drafted this report:

Christine Alex -- National Weather Service
Kenneth Allen -- Executive Director, Partnership for Public Warning
Art Botterell -- Moderator, Common Alerting Protocol Working Group
Ray Chadwick -- President, ClassCo Inc.
Joanne Donnelan -- National Center for Missing and Exploited Children
Gary Dubrueler -- Shenendoah County, Virginia, Emergency Management
Darrell Ernst -- The MITRE Corporation
Eric Forsman -- EMCOM, National Emergency Alert Notification System
Tom Hughes -- ComCare Alliance
Douglas J. Lowe -- Teledyne Brown Engineering
Frank Lucia -- Federal Communications Commission, retired
Roland Lussier – Comlabs
Kevin McCarthy -- Reverse-911
Dr. Andrew Michael -- U.S. Geological Survey
Efraim Petel -- President, Hormann America, Inc.
Kendall Post -- Chief Technology Officer, Alert Systems
Kenneth Putkovich -- Chief, Dissemination Systems, National Weather Service
Richard Rudman -- Partnership for Public Warning
Jeffrey Sands -- The MITRE Corporation, PCIS
Greg Sink -- Vice President and General Manager, Federal Signal Corporation
Rick Tiene -- Vice President, Roam Secure Inc.
Dr. Peter Ward -- Chair, Board of Trustees, Partnership for Public Warning
Stan Wentz -- Federal Emergency Management Agency
Walt Zaleski -- National Weather Service Southern Region

Each of these people participated based on their extensive experience. They do not necessarily speak for the position of their organizations.

This report has been reviewed and commented on by the following persons:

Doug Allport -- President, Allport Group
Bernice Carr -- Federal Emergency Management Agency Operations Center
Alan Clive -- Federal Emergency Management Agency, Civil Rights Program Manager
Amanda Dory, International Affairs Fellow, Center for Strategic & International Studies
Sol Glasner -- Vice President, General Counsel and Secretary, The MITRE Corporation
Mike Hoban -- Vice President, 3e Technologies International
Ken Keane -- Partner, Arter and Hadden LLP

David Larimer -- Federal Emergency Management Agency, Office of National Preparedness
Dave Liebersbach -- Director, Alaska Division of Emergency Services
Dr. Dennis Mileti -- Director, Natural Hazards Research and Applications Information Center; Chair, Department of Sociology, University of Colorado at Boulder
Jeng Mao -- Department of Commerce, National Telecommunications and Information Administration
Dr. Nancy Mock, Associate Professor, Department of International Health and Development, Tulane University
George Nichols -- Vice President, Dialogic Communications Corporation
Tim Putprush -- Federal Emergency Management Agency, Primary Entry Point Coordinator
Dr. Barbara T. Reagor -- Fellow, Executive Partner, Homeland Security & Government Solutions, Telcordia Technologies, Inc.
Ben Rotholtz -- General Manager, Products and Systems, RealNetworks
Fred Schamann -- NASA Goddard Space Flight Center
Alan Shoemaker – Director of Public Affairs, The MITRE Corporation
Lacy Suiter -- National Emergency Managers Association, FEMA retired
Ralph Swisher -- Federal Emergency Management Agency, Office of National Preparedness
Chris Warner -- Founder and CEO of Earth 911 network
George Wilcox -- Department of Commerce, National Oceanic and Atmospheric Administration, Corporate Liaison

Appendix 2: Glossary Of Terms

All-hazard: Natural hazards, technological accidents, and acts of terrorism.

AMBER: America's Missing: Broadcast Emergency Response. Immediate broadcast of information about abducted children using the Emergency Alert System, electronic highway signs, and such.

EAS: The Emergency Alert System (www.fcc.gov/eb/eas/). Operated under 47 CFR Part 11 (www.fcc.gov/eb/eas/rules.htm).

EBS: The Emergency Broadcast System. Predecessor to the Emergency Alert System.

FAOC: The FEMA Alternate Operations Center in Thomasville, Georgia.

FCC: Federal Communications Commission (www.fcc.gov).

FEMA: The Federal Emergency Management Agency (www.fema.gov).

FOC: The FEMA Operations Center at Mt. Weather, Bluemont, Virginia.

HSAS: Homeland Security Advisory System (www.whitehouse.gov/homeland/).

NAWAS: The National Warning System operated by FEMA is a 24-hour continuous private line telephone system used to convey warnings to Federal, state and local governments, as well as the military and civilian population. Originally, the primary mission of the NAWAS was to warn of an imminent enemy attack or an actual accidental missile launch upon the United States. NAWAS still supports this mission but the emphasis is on natural and technological disasters. The operations manual is found at www.fema.gov/pdf/library/1550_2.pdf.

NIAC: National Industry Advisory Committee appointed by the FCC to provide advice on the Emergency Broadcast System.

NLETS: National Law Enforcement Telecommunications System is a sophisticated message-switching network linking local, state, and Federal agencies together to provide the capability to exchange criminal justice and public safety related information interstate. The system is operated and controlled by the states (www.nlets.org).

NOAA: National Oceanic and Atmospheric Administration.

NORAD: North American Aerospace Defense Command, Peterson Air Force Base, Colorado (www.norad.mil) is a bi-national United States and Canadian organization charged with the missions of aerospace warning and aerospace control for North America. Aerospace warning includes the monitoring of man-made objects in space, and the detection, validation, and warning of attack against North America whether by aircraft, missiles, or space vehicles, utilizing mutual support arrangements with other

commands. Aerospace control includes ensuring air sovereignty and air defense of the airspace of Canada and the United States.

NWR: NOAA Weather Radio is a nationwide network of radio stations broadcasting continuous weather information direct from a nearby National Weather Service office. NWR broadcasts National Weather Service warnings, watches, forecasts and other hazard information 24 hours a day (205.156.54.206/nwr).

NWS: The National Weather Service, part of the National Oceanic and Atmospheric Administration under the Department of Commerce (www.nws.noaa.gov).

NWWS: The NOAA Weather Wire Service is a satellite data collection and dissemination system operated by the NWS. Its purpose is to provide state and Federal government, commercial users, media, and private citizens with timely delivery of meteorological, hydrological, climatological, and geophysical information (205.156.54.206/nwws).

Public warning: A public warning is a communication that directs attention to new information about a hazard or threat for the purpose of causing focused action that reduces harm. A warning may alert people to an imminent hazard or may notify them about a hazardous event that is in progress or just happened. A warning should communicate what, where, when, and how severe the hazard is, how likely the hazard is to occur, and what action is appropriate. A warning needs to communicate clearly and succinctly the risk people face, to motivate them to take specific action, and to provide guidance as to what that action should be. The success of a warning is measured by the actions people take. Public warning is a public good that is generally delivered through privately-owned communication networks and devices.

WAWAS: The Washington D.C. Area Warning System operated by Washington D.C. Office of Emergency Preparedness (coldwardc.homestead.com/files/wawas/index.html).

Appendix 3: Dissemination Possibilities

Warnings will be most effective when they can be delivered to people no matter where they are or what they are doing. Warnings must be focused on people directly at risk and/or with a need to know. There are numerous technologies to do this that either exist or are under development. America is technology enabled and this allows people to choose devices that best suit their needs with due respect to privacy. The challenge is to plan and develop interoperable standards, protocols, planning, and procedures that can effectively utilize the technology.

Mass warning devices: Warnings can be delivered to large numbers of people inside or outside of buildings using sirens, horns, public address systems, loudspeakers mounted on police cars, bull horns, electronic highway signs, flashing lights, and related devices.

Wired warning devices: Nearly all homes and offices have telephones. Warnings can be delivered by computers calling all telephones in a region or by sending digital signals on telephone lines or even power lines that activate devices to capture attention and deliver the message. The location of wired devices can be known either by the device or by a database (such as 911) to provide for geographic focusing. Many homes and offices now have security systems that could also conceivably deliver warning messages.

Wireless warning devices: New types of wireless devices that deliver information are being introduced regularly. Radio and television stations and cable systems currently broadcast warnings through the Emergency Alert System by interrupting programming. As these media move to digital formats, warnings can be transmitted that will only interrupt programming for those receivers in areas of risk or owned by people with a need to know. Warnings are already transmitted as digital codes embedded in analog radio and television signals that can activate special receivers, turning them on and announcing or displaying the emergency message. Specific cellular telephones can be called or signals can be broadcast to all cellular telephones in specific cells. Numerous wireless devices receive digital signals, including pagers, computers, pocket organizers, and wristwatches. These signals may come in Internet format or simply multiplexed into radio, television, or other types of data streams operated for reasons that may have nothing to do with warning. Rapidly increasing numbers of Americans are carrying and using electronic devices daily for reasons other than warning. All of these devices could also deliver warnings, and adding this capability can be very inexpensive. Use of GPS and other electronic location technologies allow receivers to know their location and to receive location-specific warning information from satellites, television, radio, Internet, and other sources.

Internet: The Internet is becoming pervasive, whether wired, wireless or via satellite. Internet Protocol is being used for cell phones and many other digital devices. Warning messages can be sent by email or by data packets in a variety of formats that could cause a message to pop up on the screen or trigger alerting devices. Internet overload during a crisis can be reduced by broadcast techniques and by use of “light-weight” messaging. The Internet also allows warning recipients to request more information.

Telematics systems: Devices are now being built into automobiles and other vehicles that detect an accident or illegal use and transmit signals with information on severity and location. These same systems could deliver warnings to the vehicle occupants.

There are endless possibilities for technologies to deliver warnings. Each has benefits and drawbacks. The most effective warning systems will utilize a wide variety of technologies and thereby increase the likelihood of reaching everyone at risk. Some technologies may offer precise location capabilities, others only broader location capabilities. Which technologies are most effective and most popular will be determined in the marketplace. The challenge is to empower industry by providing warning information through standardized procedures in standardized terminology and format that can be input reliably to these technologies from all authorized sources.