

# News from the Internet Society

Bulletin no. 10 - February 14<sup>th</sup>, 2005  
Also available at: [www.isoc.org/news/](http://www.isoc.org/news/)



## The 'Public Warning Network Challenge' A Call for Collaborative Action

The disaster that followed the tsunami of December 2004 has challenged providers of information and communications technologies to find ways to improve public warning. Warning systems must be able to alert the public about major hazards and should communicate warning messages via all available notification methods.

Because the Internet will play a significant role in the efficient distribution of these time-critical alerts, the Internet Society (ISOC) has launched the 'Public Warning Network Challenge' - a call for collaborative action in order to make such public warning systems a reality.

### The Challenge

**Collaborative actions are necessary to assure that standards-based, all-media, all-hazards public warning becomes an essential infrastructure component available to all societies worldwide.**

"Any organization involved in an aspect of public warning is invited to endorse the 'Public Warning Network Challenge' and indicate how they are able to collaborate on this goal," said Lynn St. Amour, President and CEO of the Internet Society. "This is an excellent opportunity to show how diverse organisations and entities, supported by the Internet, can work together to develop a global partnership for development that will enhance the safety of millions of people."

To endorse the 'Public Warning Network Challenge', please complete the form here:

<http://www.isoc.org/challenge>

The WSIS Declaration of Principles has already highlighted the need to pay special attention to conditions that pose severe threats to development, such as natural disasters. The WSIS Action Plan goes on to make a specific call to establish monitoring systems, using ICTs, to forecast and monitor the impact of natural and man-made disasters particularly in developing countries, LDCs and small economies.

To support these goals, The 'Public Warning Network Challenge' will provide an enabling environment in which stakeholders everywhere can cooperate to bring the benefits of ICT applications to the area of disaster prevention.

1775 Wiehle Ave.  
Suite 102  
Reston, VA 20190-5108  
USA  
tel: +1 703 326 9880  
fax: +1 703 326 9881  
Email: [info@isoc.org](mailto:info@isoc.org)

4, rue des Falaises  
CH-1205 Geneva  
Switzerland  
tel: +41 22 807 1444  
fax: +41 22 807 1445



The Internet Society ([www.isoc.org](http://www.isoc.org)) is a not-for-profit membership organization founded in 1991 to provide leadership in Internet related standards, education, and policy. With offices in Washington, DC, and Geneva, Switzerland, it is dedicated to ensuring the open development, evolution and use of the Internet for the benefit of people throughout the world. ISOC is the organizational home of the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), the Internet Engineering Steering Group (IESG) and other Internet-related bodies who together play a critical role in ensuring that the Internet develops in a stable and open manner.

### Important cautions

Effective public warning involves many distinct aspects not addressed here, including public education, training, building codes, policy, science, and research, among many others.

Emergency management processes should provide for human judgment between the detection of a threat situation and the issuing of public alerts, usually under control of officials with appropriate responsibilities.

Designers of technologies supporting public warning should take into account that false alarms can be disruptive, expensive, and can degrade public confidence.

In any system of public warning, the authentication of senders and targeted receivers is essential. Also, alerting systems can be targets for deliberate misinformation or denial-of-service attacks.

Where alerting involves existing operational systems, any implementation of new technology will begin in parallel with current operations to assure there is no disruption of service or source of confusion.

### Background

The goal of public warning is that people who are properly alerted will act to reduce the damage and loss of life caused by a natural or man-made hazard event. To ensure that everyone can be alerted, it is essential to leverage all available communications media. To minimize the public confusion that occurs during emergencies, the alerting system should be in routine use for all hazards, not only for rare events such as earthquakes and tsunami, but for severe weather, fire, and other threats.

Authoritative alert messages should transmit on all available communications media as appropriate, including broadcast or individual targeting. Alerts should be converted automatically and securely into forms suitable for each technology: Internet messages, news feeds, text captions on television, messages on highway signs, voice on radio and telephones, signals for sirens, etc.

In many nations, common carriers such as radio, television, and telephone networks have implemented particular public alert technologies for hazards or threats such as weather events or civil defence. From the societal perspective of public warning investments, it makes no sense to continue building a separate public warning system for each particular threat. Efficient use of funds as well as effectiveness of public warning both argue for using standards and combining the public warning requirement for all-media coverage with the requirement for an all-hazards approach.

A standards-based, all-media, all-hazards public warning strategy not only makes sense for governments who need to alert the public, it makes sense for a wide range of information technology providers and communications carriers as well.

Many activities are already underway within the Internet community. For example, a new proposal for using the Internet to quickly warn large numbers of people of impending emergencies is currently being drafted by the Internet Engineering Task Force (IETF).

The content of alert messages is now being standardized across all hazard types, including severe weather, fires, earthquakes, and tsunami. In 2004, the Common Alerting Protocol (CAP) was agreed as an international standard for all-hazard alert messages.

### For more information:

The 'Public Warning Network Challenge':  
<http://www.isoc.org/challenge>

Internet draft - 'Structure of an International Emergency Alert System':  
<http://www.ietf.org/internet-drafts/draft-baker-alert-system-00.txt>

The Common Alerting Protocol:  
<http://www.oasis-open.org/committees/emergency/>