March 2013

WORKING GROUP 2
Next Generation Alerting
Final Report

Table of Contents

1 Results in Brief

1.1 Executive Summary

The Communications Security, Reliability, and Interoperability Council ("CSRIC" or the "Council") is a federal advisory committee established by the Federal Communications Commission ("FCC" or the "Commission") to provide recommendations to the FCC regarding best practices and actions the Commission may take to ensure optimal operability, security, reliability, and resilience of communications systems. The systems at issue include telecommunications, media, and public safety communications systems. The FCC created ten Working Groups to develop information for CSRIC, and each of the groups was given a charter of responsibilities relating to a topic area.

Working Group 2 ("WG2" or the "Working Group") was established to examine next generation alerting, to explore many aspects of alerting with a focus on utilization of the Internet and other broadband-based resources, and to develop recommendations for CSRIC's consideration regarding actions the FCC should take to promote deployment of next generation alerting systems.

WG2 identified five constituencies that are likely to have stakes in the activities of next generation alerting – government and non-governmental organization alerting system operators, providers of distribution platforms, makers of receiving devices, content providers, and access and functional needs interests – and energetically recruited members from those constituencies, with the goal of informing our work and ensuring that our recommendations would take into account a diverse collection of perspectives.

WG2 also established three committees to focus on separate portions of the charter given to the Working Group by the FCC: Architectures and Platforms, Technical and Operational Criteria, and Social Media Alerting. The committees surveyed the current alerting systems, evaluated concerns with those capabilities, and identified issues that can be addressed constructively in the development of next generation alerting practices and resources. Through the efforts of the committees, WG2 examined the users of alerts and warnings, reviewed the pertinent legislative and regulatory framework affecting alerting, developed an "alert activity chain" to illustrate common alerting designs and terminology, identified areas in which standards bodies currently provide significant value in the design and operation of alerting systems and where further standards work would be beneficial, analyzed how the public reacts to messages received through official government channels as well as social media, and examined ways in which increased use of social media could provide value in delivering larger amounts of useful alert-related information to diverse groups of recipients before, during, and immediately following an emergency or crisis.

WG2 has developed recommendations for CSRIC concerning actions the FCC should take to promote deployment of next generation alerting systems involving the following topics:

- Protection and strengthening of the Common Alerting Protocol (CAP) to ensure that all participants in the alerting process can communicate efficiently as system capabilities evolve.

- Provision of funding to support the implementation and sustaining of alerting system architecture.
- Development of processes and standards to govern practices of implementing CAP.
- Supporting the rapid development of devices for recipients of alerts with improved capacities for disseminating relevant, geographically targeted alerting information.
- Encouraging creation of strategic plans for identifying and streamlining the deployment of new alert dissemination technologies.
- Special actions to promote research and development for technologies that will convey alert information effectively for individual groups within the access and functional needs communities.
- Arrangements for standardized training for emergency managers on using social media for alerting, for producing a strategic vision for creating tools that support use of social media for alerting, and for developing programs to ensure the efficacy of using the resources of social media for public alerting.
- Creation of industry advisory bodies to provide guidance for a future version of the Commercial Mobile Alert System (taking into account the advent and wide use of smartphones and the migration to fourth-generation or "4G" networks) and to develop standards for deployment of broadband alerting.
- Ensuring that deployment of next generation alerting capabilities does not exclude the continued provision of alert information via existing technologies that continue to be available (so as not to exclude users of such legacy technologies from alerts), but incorporates those technologies into next generation alert delivery methods as much as possible.

Most importantly, in recognition of (i) the ongoing development and implementation of the Emergency Alert System ("EAS") and the Commercial Mobile Alert System ("CMAS") and (ii) the continuing and rapid advances in the fields of broadband system design, content delivery, Internet applications, and social media services, WG2 believes that the FCC should create a working group as part of a future CSRIC to take into account those developments and advances in building upon WG2's recommendations for promoting deployment of next generation alerting.

2 Introduction

The CSRIC was established by the FCC as a federal advisory committee designed to provide recommendations to the Commission regarding best practices and actions the Commission may take to ensure optimal operability, security, reliability, and resiliency of communications systems, including telecommunications, media, and public safety communications systems.

Due to the large scope of the CSRIC mandate, the FCC created 10 Working Groups to assist the Council in its work, with each group being assigned to examine a specific set of issues. Working Group 2 ("WG2" or the "Working Group") was asked to examine Next Generation Alerting. WG2 officially started its work in September 2011.

2.1 CSRIC Structure

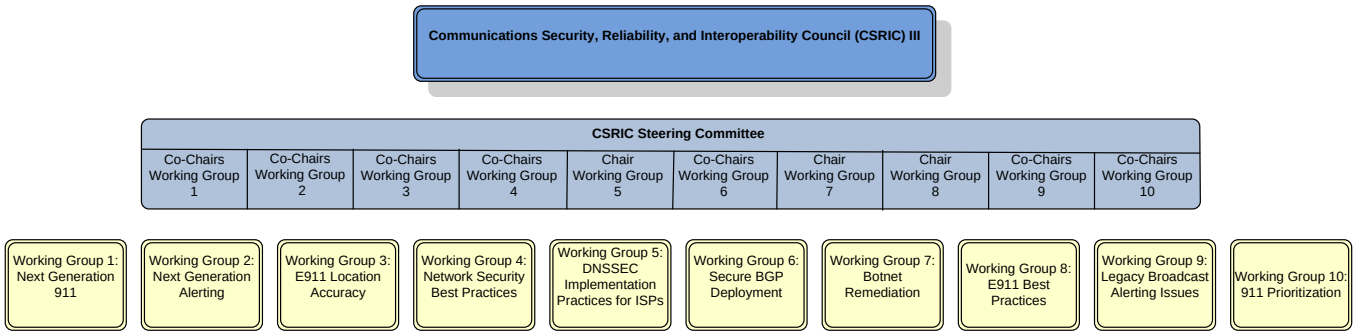

Figure 1 – CSRIC III Organization Chart

2.2 Working Group 2 Team Members

The following table lists the members of the Working Group:

Name	Company
Damon Penn, Co-Chair	FEMA
Scott Tollefsen, Co-Chair	Critical Alert Systems, LLC
Mike Adams	Cassidian Communications
Wayne Ballantyne	Motorola Mobility
Donna Bethea-Murphy	Iridium Satellite LLC
Ron Boyer	Boyer Broadband
Ann Marie Cederberg	CenturyLink
Ed Czarnecki	Monroe Electronics Inc. /Digital Alert Systems
Brian Daly	AT&T
John Davis	Sprint
Tim Dunn	T-Mobile
Mike Gerber	NOAA National Weather Service
Denis Gusty	DHS - S&T
Jorge Guzman	DIRECTV
Antwane Johnson	FEMA
Hisham Kassab	MobiLaps, LLC
Christine Kim	WG2 Support
John Kopec	Sprint
John Lawson	Convergence Services, Inc.
Kathryn Martin	Access Partnership
Christian Militeau	Intrado Inc.
Peter Musgrove	AT&T
Mike Nawrocki	Verizon
Wayne Pacine	Board of Governors of the Federal Reserve System
Jerry Parkins	Comcast Cable
Bipin Patel	Interop Technologies
Brian Rosen	Neustar
Harold Salters	Alliance for Telecommunications Industry Solutions
Andy Scott	National Cable & Telecommunications Association
Matthew Straeb	Global Security Systems, LLC

Mark Titus	TeleCommunications Systems, Inc.
Crystal Turner	WG2 Support
Christian Vogler	Gallaudet University
Larry Walke	National Association of Broadcasters
Wade Witmer	FEMA

Table 1 – List of Working Group Members

3 Objective, Scope, and Methodology

3.1 Objective

Consistent with its written charter from the FCC, the Working Group explored all aspects of next generation alerting and developed recommendations for CSRIC's consideration regarding actions the FCC should take to promote deployment of next generation alerting systems. The Working Group reviewed alerting architectures, such as those used for the Integrated Public Alert and Warning System ("IPAWS"),[1] Wireless Emergency Alerts ("WEA") (the new name for the Personal Localized Alerting Network, or "PLAN"), and the distributed architecture presented by the Internet Engineering Task Force ("IETF") Authority to the Citizen Alert ("ATOCA") Working Group.[2] The Working Group considered the manner in which these architectures, and others under development, may interoperate and interconnect to assure effective delivery of alerts. In addition, the Working Group examined different communications distribution platforms, (*e.g.*, Internet, Satellite, Digital Television ("DTV") Datacast, Mobile DTV, etc.) for alert delivery and discussed how the various architectures exploit these distribution platforms. The Working Group also explored what alert delivery media (*e.g.*, video, audio, text, graphics, etc.) can be used for the most effective delivery of next generation alerts and developed recommendations regarding how the receiving platforms (e.g., mobile phone and other wireless devices, broadcast, cable, satellite, laptops, tablets etc.) may best present the transmitted alerts to users.

In addition, the Working Group developed recommendations regarding the technical and operational criteria under which next generation alerting participants can utilize the Internet and other broadband-based architectures. The operational criteria included the relationships among different entities, including, local, tribal, state and federal governments in generating and distributing alerts. The technical requirements included consideration of the Common Alerting Protocol and other protocols for generating, formatting, and distributing alerts, as well as security requirements (including any trust models) to mitigate potential threats and attacks on the alerting systems.

Finally, the Working Group explored and developed recommendations regarding the role of social media in next generation alerting systems, including how governments may integrate social media into their own alerting systems.

3.2 Scope

Per the Working Group 2 description, the summary of assignment was to:

[1] http://www.fema.gov/emergency/ipaws/
[2] https://datatracker.ietf.org/meeting/79/materials.html#wg-atoca

1. Explore all aspects of next generation alerting; and
2. Develop recommendations for CSRIC's consideration regarding actions the FCC should take to promote development of next generation alerting systems:
   a. How alerting architectures may interoperate
   b. How architectures may exploit different platforms
   c. How various forms of delivery media may be used
   d. How receiving platforms may best present alerts
   e. Technical and operational criteria
   f. Role of social media in next generation alerting

3.3 Methodology

The Working Group used a collaborative, inclusive approach to its work. Given the vast array of expertise the group members brought to bear on this effort, it was critical to provide a multitude of forums and mediums through which participants could express their opinions and help shape this final report. The Working Group conducted monthly conference calls and held in-person meetings in Washington, DC. During the initial months of work, the Working Group arranged for presentations on the alerting systems currently in use or development, to help assure that the members had a common knowledge base for assessing alerting issues. The Working Group had speakers address additional topics at the face-to-face meetings in Washington. Members also toured facilities at the Federal Emergency Management Agency and at the American Red Cross to see alerting systems in operation. The following section details the methodology through which the group achieved this objective.

3.3.1 Sub-Group Structure

After recruiting and its initial set of meetings, the Co-Chairs decided to break the working group into three committees: Architectures and Platforms Committee, Technical and Operational Criteria Committee and Social Media Alerting Committee. Many members of WG2 served on more than one committee.

Committee 1: Architectures and Platforms. The Architectures and Platforms Committee was tasked to develop recommendations regarding how various combinations of alerting architectures, distribution platforms (transport infrastructures), and receiving platforms (end-user devices) may best present transmitted alerts to users.

Committee #1 Co-Chairs: Ed Czarnecki, Brian Rosen, Hisham Kassab
Explored topics:

1. Handling multi-media alerts in different networks
2. Adding new alert dissemination technologies
3. Access for alert originators
4. Data format(s) for alert messages
5. Adherence to digital security standards
6. Devices for receiving emergency alerts
7. User control over receipt of alerts (opt in / opt out)

Committee 2: Technical and Operational Criteria Committee. The Technical and Operational Criteria Committee was tasked to develop recommendations regarding the technical

and operational criteria under which next generation alerting participants can utilize the Internet and other broadband-based architectures.

Committee #2 Co-Chairs: Ron Boyer, Ann Marie Cederberg, Brian Daly
Explored topics:

1. Issues with communications systems and networks
2. Key information absent from current alerts
3. Techniques for geo-targeting alerts
4. Emerging technologies

Committee 3: Social Media Alerting Committee. The Social Media Alerting Committee was tasked to develop recommendations regarding the role of social media in next generation alerting systems, including how governments may integrate social media into their own alerting systems.

Committee #3 Co-Chairs: Denis Gusty, Hisham Kassab
Explored topics:

1. Understanding public response
2. Importance for access and functional needs consumers
3. Compatibility with other Internet tools

Each of the three committees held frequent conference calls. The Co-Chairs of each committee framed conversation and discussion amongst the participants. The Co-Chairs had a free hand to investigate/coordinate as they saw fit. They worked to bring members closer to consensus and encouraged open dialogue designed to find common ground. For each committee meeting, extensive notes were captured and analyzed to determine if there was overlap in the issues being discussed.

3.3.2 Collaboration via Portal

In addition to the regular conference calls and in-person meetings, an online collaboration portal was implemented for use by the participants. The portal was accessible to all Working Group members throughout the duration of their work on behalf the CSRIC. The table below details some of the most prominent capabilities featured on the Portal and how they were used by the members of the Working Group.

Document Library	Collaboration space where members posted, reviewed, and edited documents.
Forum	Open space to exchange and share various types of information regarding their activities and discussions. Committee members posted questions, suggestions, and comments by creating new forum topics, or responding to existing posts by leaving comments.
Calendar	Central location where all relevant meetings and events were announced. Members could track upcoming meetings and events.
Links	Location where external internet links pertinent to CSRIC were posted.

Table 2 – Portal Capabilities

From its inception, the portal became a useful tool for the Working Group as they shared ideas, resources, and collaborated on common documents, including this final report. Given the disparate locations from which the group members originated, having an online collaboration tool was instrumental to the successful completion of the Working Group's final product.

4 Background

4.1 Current Alerting Activities and Components

Public alerting is conducted to ensure public safety. The public alerting systems described in this document are part of this nation's larger alerting network. Social scientists and the National Oceanic and Atmospheric Administration (NOAA) post-storm studies strongly suggest that alert recipients don't often take decisive lifesaving action until the recipient validate the threat via multiple trusted sources. Thus, each system may have its advantages and disadvantages, but they are all complementary from a social science and public safety perspective. As technology evolves, continuous improvements to public alerting systems are necessary to ensure the general public is most informed about the threat described in the alert and so that appropriate action is taken in response to the alert.

4.1.1 Alert Activity Chain

A brief review of current methodologies provides a needed framework to understand various challenges presented by alerts and warnings. Figure 2 shows an alert activity chain that depicts the activities involved in transmitting an emergency alert/warning from the Alert Originator (i.e., the Emergency Manager) to the Alert Recipient (typically a citizen within the targeted community). This activity chain establishes (i) a framework for understanding how alerts are generated in a conventional manner, to assist in the analysis of next-generation alerting, as well as (ii) some of the terminology that will be used in that analysis.

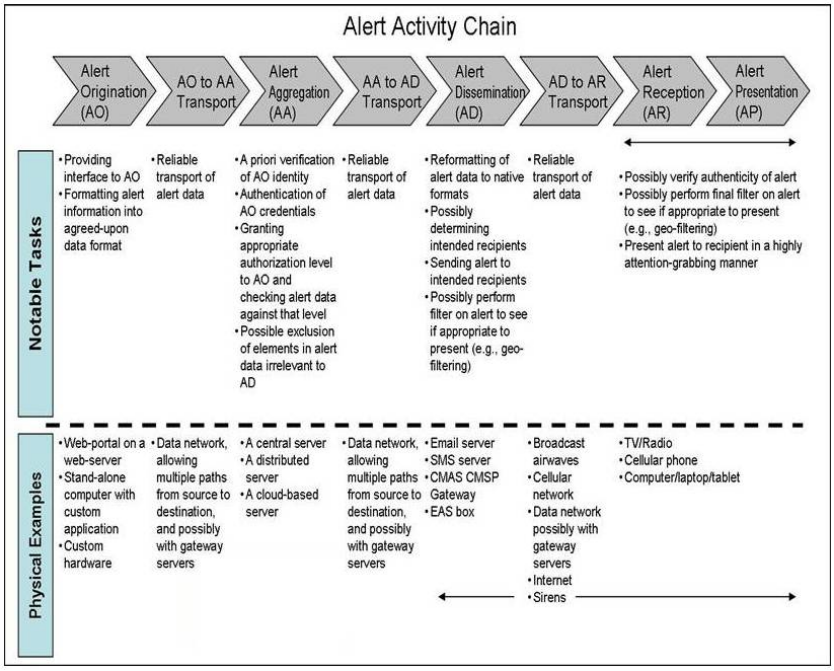

Figure 2 – Alert Activity Chain

Figure 3 shows the envisioned general-purpose architecture for next-generation alerts.

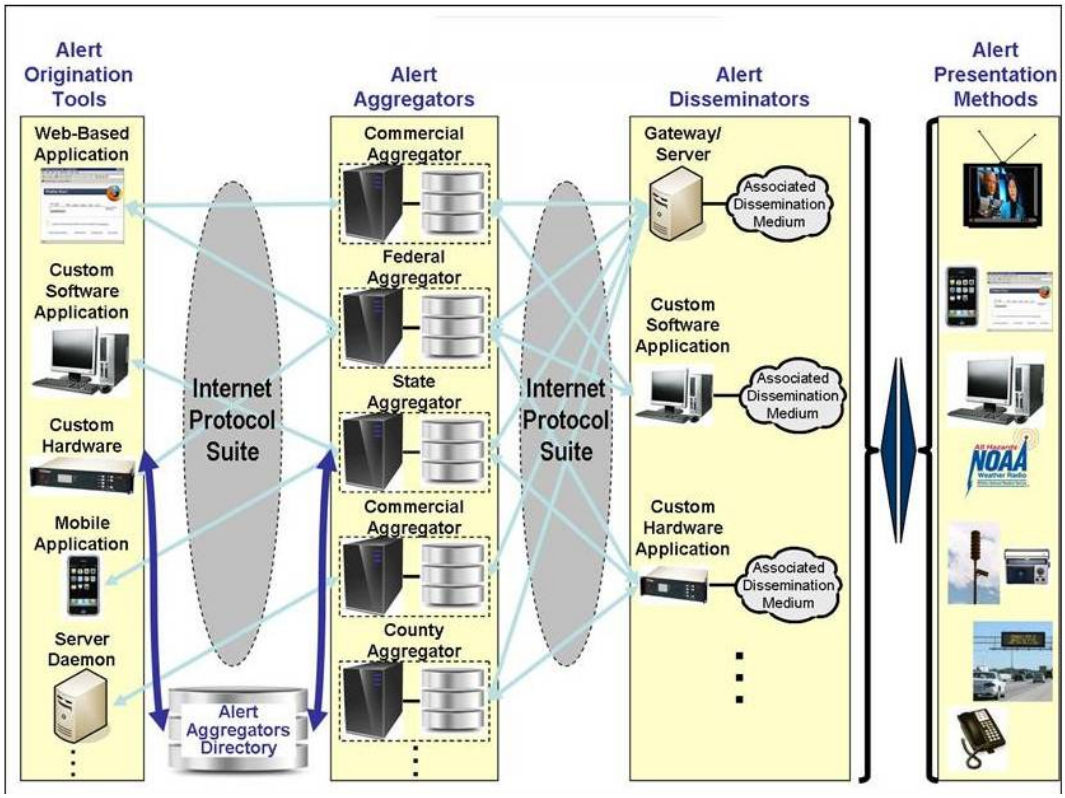

Figure 3 – Envisioned General-Purpose Architecture for Next-Generation Alerts

The set of Alert Aggregators need not be a flat structure. It can be hierarchical as illustrated in Figure 4.

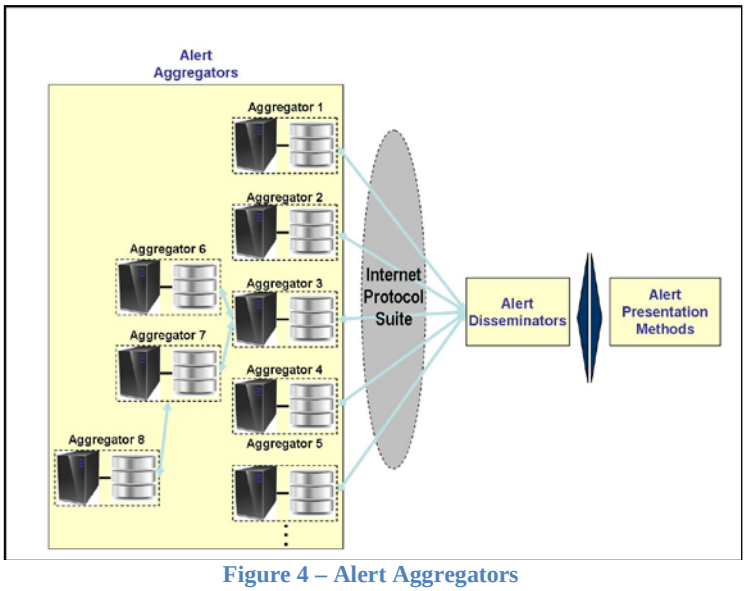

Figure 4 – Alert Aggregators

4.1.2 Current Example of an Alerting Architecture

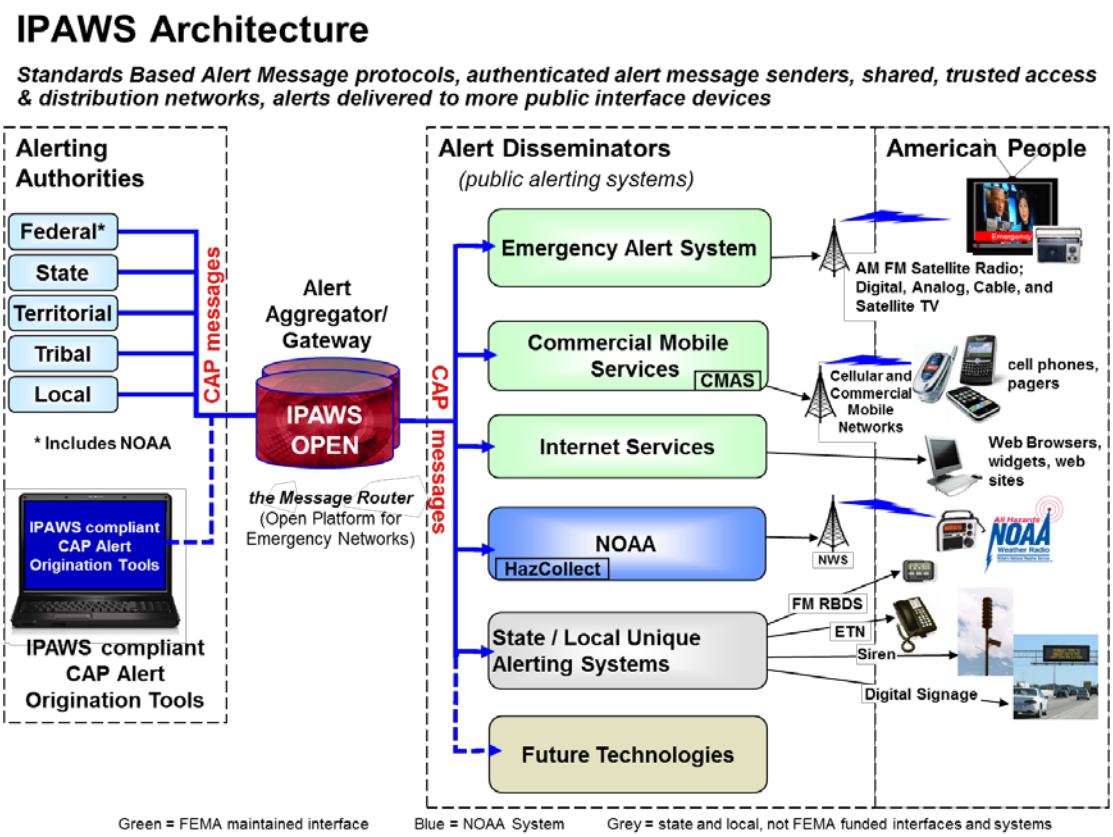

Figure 5 – IPAWS Architecture

The Integrated Public Alert and Warning System (IPAWS), whose architectural organization is shown in Figure 5, is an emergency warning system currently overseen by the Federal Emergency Management Agency (FEMA). It allows emergency managers and other alerting officials at the Federal, State, Territorial, Tribal and Local level to originate a single message and transmit it via several alert disseminators. It uses a single aggregator as a transport platform and the Common Alerting Protocol (CAP) standard to ensure system compatibility. A message is originated on the left-hand side of the illustration, processed through the alert aggregator, and disseminated over the multiple methods on the right. The concept allows the use of existing technologies that state and local governments may already have, as well as leaving the door open for the development of future technologies.

IPAWS is used here as an example only. It is not the intent of this report to improve or redesign the current system, but to show how the architectural organization described above can be and has been put to use in an actual system.

4.2 Challenges of Existing Systems

There are many limitations and constraints on existing systems. For brevity, we will use the IPAWS model to highlight issues common to existing technologies.

4.2.1 What limitations exist in the IPAWS Network that effect In-Field Operations?

1. Reliability/Resilience: The most common limitation for existing systems is the risk that the system may not function seamlessly, under all conditions. IPAWS and related systems are subject to natural (wind, flooding, fire, cold and earthquakes) and human caused (acts of war, terrorist and cyber attaches) events which could interrupt the ability to send and deliver alerts. In evaluating the proposed functionality and mission critical nature of the CAP/IPAWS system, it is believed that the server facility should be designed with minimal points of failure. Current systems have no "industry standard" and no Federal or State regulation. No hardware certification process, other than CAP recommendations, governs manufacturers and no third party testing facility exists to enforce standards once fully developed.

2. Alert Verification: As the current CAP/IPAWS system is a "pull" only configuration, there is no verification method incorporated in the data stream, which results in an operational limitation. The EAS client needs a "check-and-balance" audit system to verify alert status. No process exists to create audit trails that allow the alert initiator to verify whether alerts have been sent.

3. Adherence to industry standards: It is important that all external network interfaces adhere to industry standards In order to allow the utilization of standardized hardware, and to ensure the longest life cycle of the network. No program exists that encourages continued maintenance of products and product developments as capabilities expand.

4. Geographically targeting specific areas: Some alerting systems which receive their alerts from IPAWS are unable to limit the geo-targeting of the alert to the actual threat area defined in the CAP message (alert areas in CAP may be defined by county, polygon, or circle). For example, NOAA outlines the alert area by polygon which is often at the sub county level. However, FCC regulations for CMAS only require alerts to be broadcast at the county level, and some systems like IPAWS can target alerts to specific counties. Even then, certain counties cover hundreds of thousand square miles. In these counties, it is not uncommon for the actual alert area (e.g., Tornado Warning, Flash Flood Warning, etc.) to cover only a very small fraction of the county. When such alerts are geo-targeted to an area well beyond the actual threat area, they overreach the intended audience and subject many citizens to a false-alarm syndrome. That is, citizens outside the actual alert area become de-sensitized and are less likely to take lifesaving action in response to future alerts. Additionally, there are areas throughout the nation which have limited access to alerts, such as some mountainous locations and territorial waters.

5. Access and Functional Needs Community: Currently most systems lack the ability to incorporate fully existing and emerging technologies for alerting the aged and disabilities communities. The ability to handle external audio and video files is not defined. Additional functionality is needed to ensure that these entire communities are alerted.

6. English as a second language: Currently most systems lack the ability to alert and warn members of our population that do not speak English as a primary language. There is a need to establish a process by which additional languages can be added at the point of message origination, aggregation, or dissemination to translate the message.

7. Enforceable hardware approval policy: The key to success of the CAP/IPAWS system is standardization of network components. In order to guarantee this, the client hardware needs to meet an established technical specification. There is a need for a defined policy which will include specifications related to hardware requirements and what the current certification represents. Hardware can include, but is not limited to, decoders, encoders and edge devices.

8. Additional Operating Policies need to be created. Under the current IPAWS system, message originators are required to take training and pass an exam on how to originate effective alerts and warnings. But there are no requirements for this training or any other certification for other existing or future systems purchased by state and local message originators. Furthermore, no standards exist for such training.

4.2.2 Enhancements and Emerging Technology

4.2.2.1 Emerging Technologies

The most difficult tasks associated with emerging technologies are determining how to integrate systems and technologies into existing systems effectively, and how to determine if out-of-date systems need to be discarded for more effective solutions. The following are some dimensions of these tasks.

1. How do we integrate future technology into existing systems?

Establish an on-going joint use taskforce consisting of both public and private participants that is charged with keeping up with new technology and application development would help mitigate these problems, so that planned enhancements to the current alert origination and distribution networks will be available. Standards should be identified.

2. Working with Intellectual Property (patents)

Advancement in areas such as social media and geo-targeting can be handicapped by patent holders and their unwillingness to allow patents to be utilized on a fair reasonable and non-discriminatory arrangement. The use of Standards and Accredited Standards organizations which have an appropriate intellectual property policy may assist in this issue.

3. What network technologies will possibly converge?

Convergence will occur as technology continues to mature and develop, and a process or policy needs to be in place to minimize alert duplications and confusion by the end users. Procedures must be developed for managing changes, eliminating multiple or duplicate alerts and providing for prioritization of alert data.

4. What technical standards can be added or enforced to maximize efforts?

There are currently multiple on-going technical standards efforts related to the communication of alerts and warnings. These efforts should be studied and their recommendations incorporated into future systems to the extent that they articulate best practices or constructive advances.

OASIS (Organization for the Advancement of Structured Information Standards) maintains the Common Alerting Protocol (CAP) within the Emergency Data eXchange Language (EDXL) set of standards. The Emergency Management CAP Sub Committee is responsible for the ongoing

management of the CAP standard and related work. See: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency-cap.

The Internet Engineering Task Force (IETF) Authority-to-Citizens Alerts (ATOCA) Working Group is working on a draft document that "provides terminology, requirements and an architectural description for protocols exchanging alerts between IP-based end points". See: http://tools.ietf.org/wg/atoca/charters.

The Alliance for Telecommunication Industry Solutions (ATIS) and Telecommunications Industry Association (TIA) are both accredited by the American National Standards Institute (ANSI) as standards developing bodies and are jointly working on interface standards for alerts and warnings to cellular networks and devices.

Additionally, the International Telecommunications Union (ITU), Open Geospatial Consortium (OGC), European Telecommunications Standards Institute (ETSI), and the 3rd Generation Partnership Project (3GPP) are working on standards and recommendations related to the communications of alerts and warnings.

4.2.2.2 Enhancements and Additional Functionality

1. Presidential National Alert, Emergency Action Notification (EAN): IPAWS can currently broadcast an EAN over EAS and send a Wireless Emergency Alert (WEA) via CMAS that informs that a Presidential Alert has been issued that citizens can hear the content of on radio and TV stations. Other than EAS and CMAS via IPAWS, current technologies do not support transmitting Presidential National Alerts over multiple alerting systems. Future systems must correct this problem by aggregating alerts over all alerting systems.

Alternate languages: As requested by the Presidential Executive Order 13407 (Section IV), a method should be incorporated in to the CAP/IPAWS system that allows for a modular approach when support for additional languages is required. IPAWS (which uses the OASIS Common Alerting Protocol, Version 1.2, with additional constraints defined in Common Alerting Protocol, v.1.2 USA Integrated Public Alert and Warning System Profile Version 1.0) includes the capacity to receive and pass on alerts in multiple languages using additional <info> blocks in a CAP message per the specifications. The rules for EAS allow for a station to broadcast alerts in the primary language of the EAS Participant and there has been some support for this capability to be present in CAP enabled EAS equipment. This initial capability is dependent upon the generator of the alert supply alternate or multiple language information in the CAP message and the participating EAS station to have equipment configured to read the CAP message, chose the alternate language, and broadcast the additional language content provided.

2. Individuals with disabilities and/or certain effects of old age: Establish what is needed to compensate for or reduce the limitations of these conditions in relation to being aware of and comprehending alerts. Establish support for audio, video, and text media. Establish procedures for ensuring that the information presented in all available media is consistent and intelligible. Establish contingencies for situations when media types are missing, or are unsupported by the available technology. Establish what is needed to ensure that the devices,

through which alerts are received, are accessible, available, and affordable to people with diminished sensory capabilities or other disabilities.

For example, not all members of the blind community have phone accessibility; in fact, there are very few devices in that market that meets this group's needs. If one is blind and receives an alert through TV or video, or if one is deaf and receives an alert through radio, the device must actually display the textual component of the alert, such as captions. With EAS today, one needs to buy a special radio that displays the alert code, and such a radio is not in widespread use. In other cases, the required equipment can be very expensive. If one has a motor disability, one needs an alert receiver device that doesn't require much dexterity to use.

There is precedent at the FCC for taking steps to address these considerations, including the following:

- The National Deaf-Blind Equipment Distribution Program, which started in July 2012 and is overseen by the FCC, and which ensures that the deaf-blind community can afford the equipment they need to participate in telecommunications
- Section 717 of the CVAA concerning phone accessibility for people who are blind or have low-vision.
- Section 203 of the CVAA, which addresses captions on small devices and hearing aid compatibility of phones, to ensure their suitability for persons with impaired hearing.

3. Specialized: Large Public Gatherings including campuses, business enterprises/facilities, stadiums, etc. present special circumstances for providing alerts to many people at a single venue, such as the benefit of alerting all persons at the same time, so as to facilitate an appropriate and coordinated responsive action from the entire group Additional functionality should be added to the alert at the origination and/or distribution network to enable the support of such special challenges. Procedures and equipment are needed that provide mobile and flexible solutions in these cases – for example, public address systems at such venues that can transmit alerts with reduced human interaction.

4. Standardize: The "look-and-feel" of alphanumeric alert content must be consistent. As devices capable of receiving and notifying the public of an alert increase in number and type, consideration should be given to establishing an alert template that will structure the alert content, thereby minimizing confusion to the public when an alert is received. A standardized template for emergency managers would minimize the possibility of confusion on the part of the alert message recipient by standardizing the form of the message that the public receives, regardless of the alert distribution network or device used.

5. "Polling" (pull) versus "Push" technology: Consideration should be given to looking at the overall data flow configuration. Evaluate expected network traffic with a focus on the potential enhancements and determine whether "pull vs. push" technique is robust enough for the future needs.

An example of a client "PULL" communication model is where the client is responsible for getting the most up-to-date information, or initiating the communication to the server. The PUSH model of communication is becoming very popular for real time data such as EAS Alerts. When the information must be delivered in real time, only the server knows when the information becomes available. The server must "PUSH" the data to the client even though the client is not polling for them.

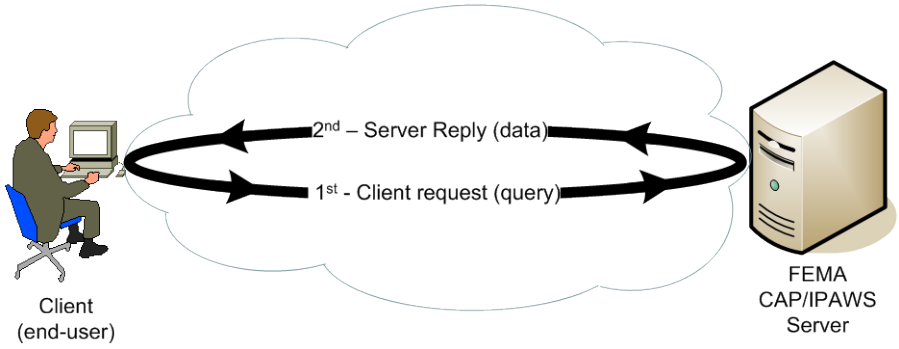

Figure 6 – Poll (pull) Data Illustration

Frequent pulling (polling) can turn into a scaling problem when many concurrent users try to capture all updates when they occur.

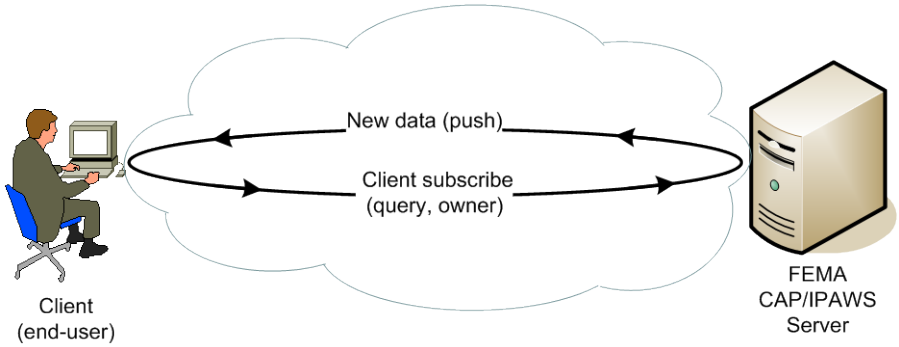

Figure 7 – Push Data Illustration

The push-based architecture illustrates an improved approach. First, an initial subscribe request is issued. This contains a query and a (client) owner address. The query is equivalent to a pull request, but can contain push-specific preferences such as pull-frequency or delivery at specific times or rates. Next, the wrapper is activated, which pushes updates whenever they happen or exactly when the user wants them delivered.

6. Expansion/modernization capability: As the State and local governments start to understand the benefits of a standardized system like CAP/IPAWS, they may want to establish their own CAP/IPAWS servers. If guidelines for designing such systems are created, then the process of establishing State and local CAP/IPAWS server systems will proceed with greater efficiency. There must be a method to establish local network solutions from a standard model that incorporate distributed local servers, to create network operational tools that enable better network management and interface to the National Server.

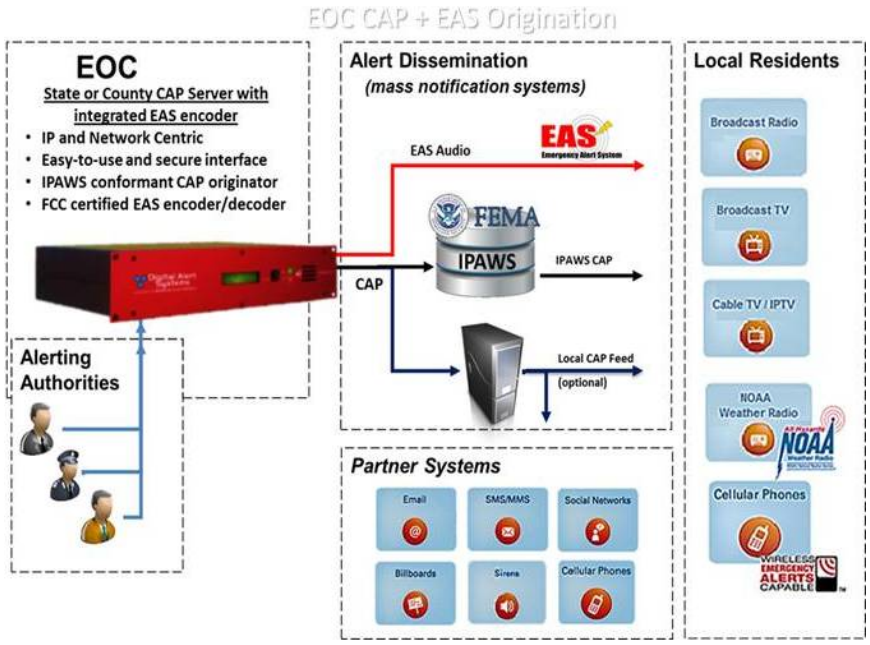

Figure 8 – Expansion Illustration

7. 3rd party enhancements: Guidelines must establish best practices and interface requirements for 3rd party providers that want to incorporate an alert relay in to their services. A method to provide additional data relevant to the subject of the alert that alert initiator or application developers can access to enhance the end-user's experience is needed. An example would be providing web URLs connecting to video, audio or data files about the circumstances that prompted the alert or about the response to those circumstances over time. Security issues regarding the URLs and trusted information source must also be addressed. IPAWS includes the capacity to receive and pass on alerts containing URLs using additional <info> blocks as specified in the CAP standard and IPAWS CAP specification This capability is dependent upon the generator of the alert supplying the URL in the CAP message and the alert distributing device or network having the capability to make use the URL.

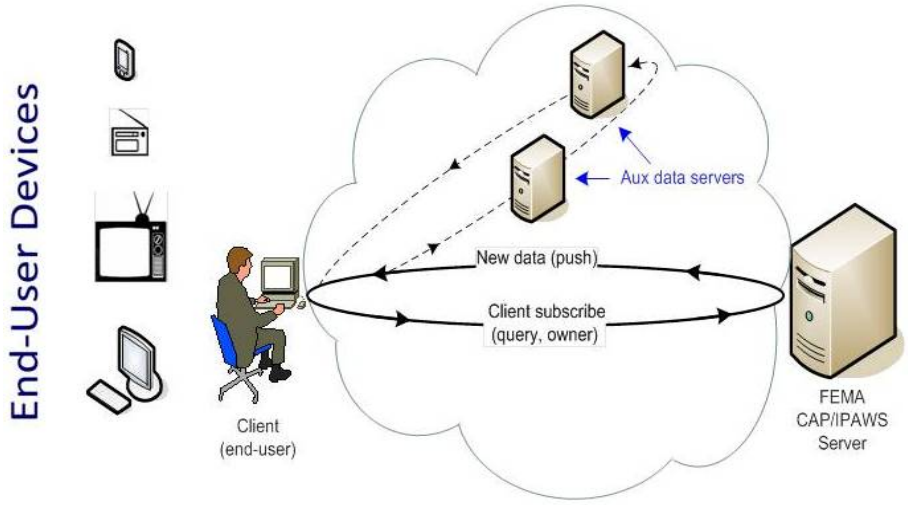

Figure 9 – Illustration of Aux 3rd Party Servers

Refer to Working Group 2, Sub-Committee 1 & 3 for additional information

8. Techniques for geo-targeting an alert to a specific area impacted: As the introduction of GPS handheld devices and mapping software improvements, it has become possible to provide more granular resolution as to the geographic area to which the alert should be addressed. Social scientists and NOAA/NWS Service Assessments have concluded that the general public responds to alerts when they feel the alert is relevant and they've received the alert from multiple trusted sources. Warning effectiveness can be greatly increased by geo-targeting the alert to the actual threat area. The converse is also true, in that poor geo-targeting of alerts can result in a false-alarm syndrome where the public becomes de-sensitized to future alerts. Polygon-based warnings can be created using alert origination software which allows the alert author to outline the alert area by connecting multiple points. According to NOAA (see http://www.nws.noaa.gov/sbwarnings), polygon-based warnings can reduce warned area by 70% to 97%, especially in the larger counties of the Western U.S.; see figure 10.

9. Also, current hazard prediction models can identify potentially affected areas based on weather conditions and the expected spill or hazard. From this, they can produce a downwind hazard message. Technology development should be encouraged to allow the identification of affected areas and the automatic transmission of a warning message without the intervention of the alert originator.

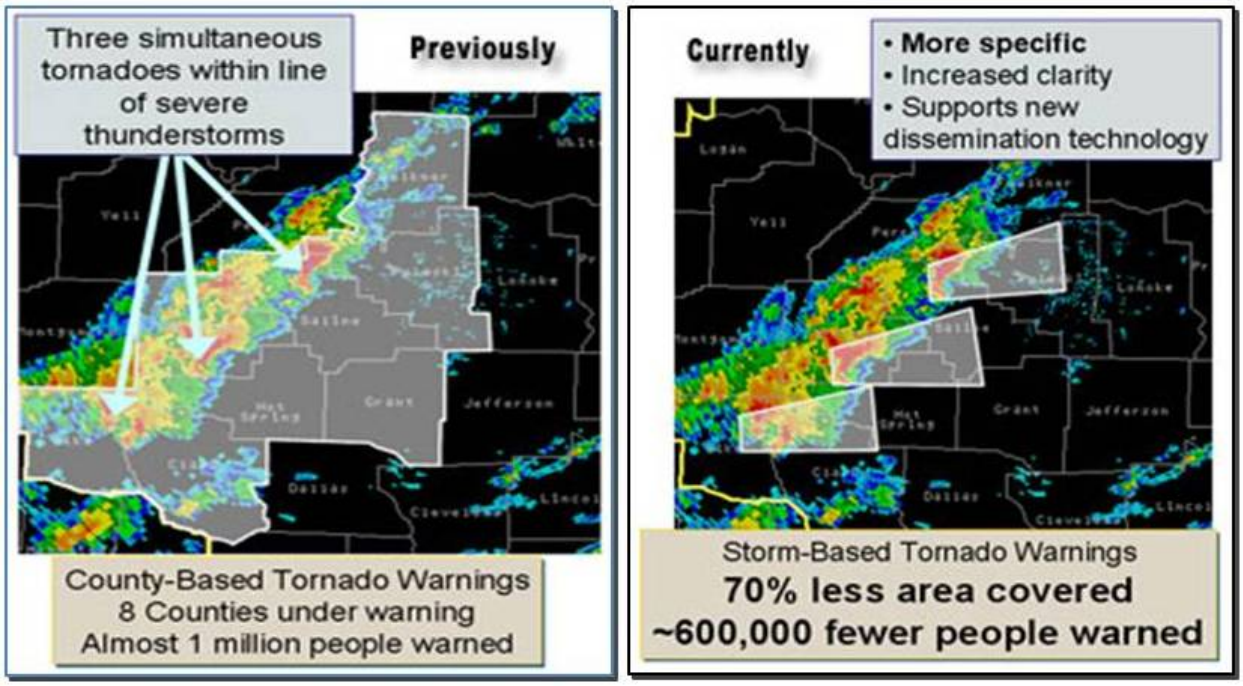

Figure 10 – Example of Alert Coverage Improvement by the Use of Polygons

4.3 Technology Solutions and Applications

4.3.1 Technology Overview

The following table identifies key communication technologies that are being utilized in the dissemination of today's emergency alerts.

	DESCRIPTION	**TECHNOLOGY**	**APPLICATIONS**	**LIMITATIONS**
A	Over-Air Radio (Analog)	Radio Frequency (RF) Off-Air - Amplitude Modulation Frequency Modulation broadcast (down-stream only), using off-air receiver	Analog audio limited text, limited signal frame video, NOAA Weather Radio	not selective, one-way, no geo-coding
B	Over-Air Radio (Digital)	Digital modulation	Active alerts, multiple-channel digital audio, text, still images, data files	Limited selectivity, one way
C	Off-Air Television (Broadcast)	RF Off-Air – Digital Modulation broadcast (down-stream only) – using off-air receiver	Digital video	not selective, one way, no geo-coding
D	Tele-Communications (Plain Old Telephone, POTS)	Close medium (fiber, twisted-pair), tethered handset (bi-directional)	Digital voice Emergency Telephone – Notification (ETN) DSL (data) VDSL (video)	Tethered, limited bandwidth
E	Multi-Channel Video Programming Distributor (MVPD) (e.g.: Cable Operator, FIOS, U-Verse, etc.)	Coax cable, Fiber optics, Wireless Broadband (WiFi), addressable set-top, cable modem (DOCSIS), bi-directional	Analog Video (one-way only) Digital Video, Data, VoIP, Video (two-way)	Tethered, limited geo-targeting Wireless – limited geo-targeting
F	Tele-Communications (Mobile Phones) using data services	Commercial Mobile Radio Service (CMRS), RF addressable digital transmission, services using an addressable wireless handset (bi-directional)	Digital Voice/Data /Mobile Apps Examples of Service providers are: Verizon, AT&T, Sprint, T-Mobile	Incomplete coverage, possible congestion.
G	Tele-Communications (Mobile Phones) using CMAS	Commercial Mobile Radio Service (CMRS), RF addressable digital transmission, services	Examples of Service providers are: Verizon, AT&T, Sprint, T-Mobile	Incomplete coverage, has 90 character limit, alphanumeric text

		using cellular broadcast (downstream only)		only, no URLs or "click through" numbers allowed.
H	Satellite Transmission (MVPD, e.g. DIRECTV), (ST-ISP, e.g. HughesNet)	Satellite digital RF transmission, limited 2-way capability, limited bandwidth, geo-targeting via one way broadcast combined with GPS in device	One-Way Digital Video (MVPD) Two-Way Data (ST-ISP), text voice, digital	Weather fade, limited filtering, high latency.
I	Iridium, Sirius SM, TerreStar	One way broadcast combined with GPS in devices	Text, voice, digital	No latency and limited weather impact

Table 3 – Key Communication Technologies

Radio Frequency (RF) for the purposes of this table should be considered transmitted through free air (broadcast).

4.3.2 Service and Applications Overview

The following table lists services and applications that are or can be utilized for dissemination of emergency alerts.

	DESCRIPTION	**TECHNOLOGY USED***	**APPLICATIONS**	**KEY LIMITATIONS**
	SMS or E-Mail	D, E, F, G	Internet	Congestion, security, reliability
	Public Alert Radios – NOAA Weather Radio	A	Weather Alerts, Emergency Alerts	One-way, no video, limited geo-targeting
	Active Alerts	B	Multi-lingual audio and text alerts	One-way
	Emergency Telephone Notification e.g. Reverse 911TM	D, E	Telephone (landline)	May not work universally with mobile phones**
	Commercial Mobile Alert System (CMAS)	F	Mobile Phone and Pagers	Subject to radio propagation
	Social Media	D, E, F, G	Facebook, Twitter, etc.	No geo-targeting
	2-Way Data (broadband)	D, E, F, G	Websites	Congestion, security, reliability
	One way Satellite Broadcast with GPS in Device	D, E, F	Mobile Phone, Computers, Auto (any device with	Urban canyon

			battery and GPS)	
	Mobile EAS (M-EAS)	D, E	Mobile Phone, Tablet, and other wireless devices	No yet enabled on most mobile devices

Table 4 – Services and Applications

* A – Analog Radio Broadcast, B – Digital Radio Broadcast, C – Television Broadcast, D – POTs, E – MVPD Services, F – Mobile Phones, G – Satellite – ISP (only) ,
** Electronic Tandem Network is not aware of the real time location of the mobile device, therefore may use owner's billing address as point of location.

4.3.3 Description of Technology and Limitations

1. Off-Air Radio Broadcast (Analog): This technology is utilized as a broadcast medium, therefore it would not be considered practical for providing the geo-targeting needed for customized alerts intended for persons in limited areas. In broadcasting, all alerts are sent to every tuned receiver in the reception area, limited by only transmitter power and terrain (except in the case of FM Radio Subcarrier alerting for RDS and HD Radio, whereby the broadcast medium has an ability to wake up and address the receiver with targeted alerts). Generally, broadcast technology might be considered the most robust because of its ability to do complex multimedia distribution of voice and data. Congestion is not an issue in a broadcast medium.

2. Off-Air Television (Broadcast): This technology is utilized as a broadcast medium, and the analysis is the same as for radio broadcasting.

3. Off-Air Digital Television, utilizing the Mobile DTV (MDTV) technology already deployed at over 130 U.S. television stations, can support geo-targeting. Utilizing an MDTV application called Mobile EAS; CAP geocodes can be pushed over broadcast Mobile DTV to an MDTV-enabled cellphone, tablet or other mobile device. The MDTV receiver can compare the alert geocodes to user configurable geo-location information and determine if the user should be notified of the alert. The alert geocodes can also be used to overlay the alert area on the device's built-in maps and provide additional rich media related to the warning. Portions of the text content in the CAP message can also be displayed.

4. Tele-Communications (Plain Old Telephone, POTS): This technology has several limitations; one being it is considered a "tethered" distribution medium. It does have one excellent attribute in that it can utilize geo-targeting information effectively (Reverse 911TM), allowing for advanced customization of the alerts received by the end-user. Congestion may be an issue.

5. MVPD Services: This technology primarily utilizes a tethered medium. With the advancements in MVPD system technologies, limited wireless (Wi-Fi) capabilities are now also being deployed. Theoretically, currently deployed technology may be capable of limited geo-targeted alerts; however, billing and operational support systems are not designed to support this type of information distribution.

6. Tele-Communications Mobile Phones/Smartphones: This technology is being recognized as the possible emerging leader in providing the most flexible distribution network when it comes to allowing the end-user the ability to utilize both pubic alerting (CMAS). CMAS is limited to 90 text characters and is a hybrid-broadcast form of RF distribution, in that it sends the alert to a geo-located cell site and the alert is broadcast from there. This provides for the effective geo-targeting of the alert. For SMS, email, or other subscription based alert distributions, congestion may be an issue for the private alerting services.

7. CMAS could take advantage of broadcast technology improvements and be enhanced to support an improved filtering ability in the handset, utilizing, for example GPS. This would further improve the geo-targeting of the alert to the end-user.

8. Satellite Transmission (MVPD and Broadcast), (ST-ISP): Utilizing satellite RF communications causes this type of technology to be a niche solution. It is considered a tethered network with limited or no up-stream capabilities. Primary mode of operation is broadcast on the downstream, limiting its geo-targeting capabilities. However, combining a satellite receiver and GPS in common devices, Satellite broadcast becomes a highly effective geo-targeted alert system with territorial coverage, no limit on alert capacity, geo fencing, and maintaining alert delivery during most conditions.

9. Mobile Applications: Hundreds of free and fee-based mobile apps have emerged for public alerting. According to a survey conducted by the American Red Cross (see http://www.redcross.org/news/press-release/More-Americans-Using-Mobile-Apps-in-Emergencies), mobile apps now tie social media as the fourth-most popular way to get information in an emergency, following TV, radio and online news. The Red Cross survey found that 20 percent of Americans said they have gotten some kind of emergency information from an app, including emergency apps, those sponsored by news outlets and privately developed apps. Some developers of mobile alerting apps get their content from official and timely sources, such as IPAWS and NOAA feeds. Other developers may "scrape" content from official or unofficial web pages which are less reliable and less timely than through official feeds. Federal and/or industry programs could be established to certify mobile apps which obtain information from official sources. Such programs might be optional for mobile app developers, but a "seal of approval" from the program could be used to encourage participation.

4.3.4 Future Dissemination Technologies

The members of WG2 wanted to avoid the exercise of predicting specific alert dissemination technologies within next-generation alerting. However, three dissemination technologies loom large, making them worth highlighting in this report:

1. CMAS: Technically, CMAS is not a future alert dissemination technology, because it was already launched in 2012. However, aspects of CMAS are still in development and could therefore be modified to take into account elements of next-generation systems. Many of the technical parameters of CMAS are governed by FCC rules (47 CFR Part 10), which themselves were formulated based on the recommendations of the FCC's Commercial Mobile Service Alert Advisory Committee (CMSAAC), a body made up of technical

experts. CMSAAC completed the bulk of its advisory work by 2007, before the advent of the smartphone as it is known today. CMSAAC envisioned CMAS to be a "bell-ringer" or source of initial information about the subject of an alert, making the ninety-character limit on message lengths quite acceptable. However, as the emergency management community became more aware of CMAS and the smartphone industry advanced over the last couple years, many have expressed dissatisfaction with the ninety-character limitation. Many also feel that CMAS's geo-targeting capability should be more precise. Emergency managers now are viewing CMAS through the lens of a revolutionized mobile device market that is dominated by smartphones and sophisticated mobile apps.

2. Broadband Alerting: Broadband Alerting was specifically mentioned in FCC's 2010 National Broadband Plan as medium that can provide the public with new ways receiving emergency information. However as detailed in Appendix F, one of the main challenges to encouraging/promoting Broadband Alerting technologies is the lack of a clear definition of Broadband Alerts. Appendix F lists several technologies, some of which are present today, that arguably qualify as Broadband alerting technologies.

3. Mobile Emergency Alert System: The new Mobile Emergency Alert System (described further in Section 5.1.2 below) is designed to leverage mobile digital TV broadcasting to deliver reliable, rich media alerts anywhere, anytime. Mobile digital TV broadcasting enables consumers to watch live television on their laptops, smart phones and other mobile devices, using an existing broadcast signal and without using the bandwidth of wireless providers. Mobile digital TV broadcasting remains nascent in the U.S., and the degree to which the Mobile Emergency Alert System will be prevalent is highly correlated with the future penetration of Mobile digital TV broadcasting in the U.S. market.

5 Architectures Development Opportunities

5.1 Standards, Protocols, Policies and Procedures

5.1.1 Authorization and Authentication of Alert Originators

It is important that only authorized individuals/organizations be able to send out emergency alerts to the public. Across the country, there are thousands of federal, state, local, and tribal governmental entities with designated individuals or organizations that would be entitled to send out emergency alerts under the authority of the respective government(s). Additionally, there are non-governmental individuals and organizations (such as day-care providers and chemical plant safety officials) that are able to send alerts over private networks owned or controlled by such persons or entities. While these individuals and organizations have no authority to transmit alerts on behalf of the government, some would urge that they should be able to send out alerts to concerned citizens.

In the cases above, the potential audience for the alert needs to be commensurate with the jurisdiction and/or the scope of the responsibilities of the Alert Originator; while allowing the possibility of escalating the alert. For example, a county emergency manager need not have the authority to send out an alert to the entire state, but if deemed necessary, he or she can contact the state emergency manager (preferably through a hotline) to send out an alert across the state. Ensuring that only authorized individuals send out alerts is a multi-step process, which includes

at the least the following elements:

- A priori verification of identity, responsibilities and jurisdictional authority – this step is probably easier to execute for government officials/organizations than for non-governmental entities/individuals.

- Determination of alerting-powers parameters e.g., geographic scope and access to certain dissemination channels such as EAS.

- Issuance of authentication credentials.

- Real-time verification of authentication credentials and adherence to alerting-powers parameters.

It would be a monumental task for a centralized office/program to perform all of the steps above.

5.1.2 Recent Innovation in Alert Dissemination Technologies

Other than CMAS, new AD technologies in recent years (e.g., SMS alerts) have primarily been commercially driven (i.e., for profit). However, as demonstrated by the CMAS example, not all society-benefiting alerting technologies will emerge via entrepreneurial forces alone. Governmental shaping and intervention is probably needed more if the goal is to deploy the new AD technology nationwide. This is again demonstrated by the contrast of the CMAS example (which is heading towards comprehensive nationwide deployment) vs. the SMS example (which has been used in limited or isolated locations).

Since certain systems need licenses, the federal government can rely on regulation to shape the deployment and use of such systems, but this is not the only path. As one alternative, participation in CMAS by wireless service providers is voluntary, although nonparticipating providers are required to post a notice of nonparticipation at each point-of-sale and to give a similar notice to the provider's existing customers.

The Mobile Emergency Alert System (Mobile EAS or M-EAS), nearing final standards adoption by ATSC, rides on top of the broadcast Mobile DTV signal to provide alert and warning. It combines the reach and bandwidth of broadcasting with the immediacy of mobile communications. Geo-targeting is an integral part of Mobile EAS, as is the ability to simultaneously deliver alerts and rich-media content to an infinite number of receiving devices in a signal coverage area. M-EAS is delivered to mobile devices independently of the cellular network, which can dramatically increase the reliability of mobile alerting, provided that citizens in the targeted area have devices capable of receiving the MEAS broadcast. Although it has been discussed, the M-EAS architecture and demonstrations to date have not shown the use of CAP based alert messages or integration with a CAP aggregator such as IPAWS.

After a successful pilot project, a number of broadcasters plan to begin operational deployment of M-EAS in the second quarter of 2013. However, mass deployment of M-EAS depends upon inclusion of Mobile DTV tuners in mobile devices. This may be a policy area that the FCC should examine closely with the goal of formulating policies that could spur development.

At least one industry participant leverages online advertising technology to receive and transmit detailed information about emergencies to Internet browser display space used for advertising. However, there is a cost associated with each alert pushed to the display space as it relies on advertising and pop-up/ad blockers can preclude the alerts from being displayed.

A representative of this industry participant describes the service as follows: Numerous websites already have browser display space embedded in them. Internet banner display network technology allows real-time geo-targeted dynamic messaging through the existing Internet browser in desktop and mobile devices and can utilize advertising technology to target the user in the impacted area. The underlying technology has improved over the past five years. Real time advertising bidding (RTB) can bid, like an auction, in real time on geo-targeted user impressions through the browser on behalf of advertisers. Thus, emergency messages can interrupt online display advertising on a specific web page being visited by a person in the threat area. The technology is only triggered when a person opens a browser on a website when it has display space for advertising. Technology can create the warning message within milliseconds through dynamic rendering technology to produce alert banners that are standard sizes as determined by the online advertising industry. When the user clicks on the emergency banner, the user is taken to the full details of the alert. In the case of a Presidential message or any other category of alerts given priority, the technology could be used to interrupt online advertising nationwide and display the message.

5.1.3 Assumption of CAP Data Format

The Common Alerting Protocol (CAP) has emerged as the dominant data format for exchanging digital public warnings and emergencies between disparate alerting technologies. It is based on the Extensible Markup Language (XML). The effort of creating the CAP specification began in 2001 by a group of 100+ independent emergency managers. Eventually the development of the standard was formalized via the OASIS (Organization for the Advancement of Structured Information Standards) standards process, while continuing to involve a large number of subject matter experts from various stakeholders in the emergency alerting community.

Given the genesis and the long history of the CAP specification's development, it is reasonable to assume that it captures the needs of the alerting community to a large extent, and that starting a competing specification would entail a fair amount of wheel reinvention. As alerting technologies, communication technologies and communication devices evolve, it is unlikely that CAP in its current format will satisfy all the needs of the emergency alerting community – it needs to continually evolve to keep up with those needs.

5.1.4 Support of New Data Types in CAP

Although based on XML, the extensibility of the CAP standard (Common Alerting Protocol Version 1.2, OASIS Standard dated 01 July 2010) and the specification for interoperation with IPAWS (CAPv1.2 USA IPAWS Profile v1.0) is limited by the standard and specifications. For example, the IPAWS Profile specification restricts CAP to a defined set of fields that can be used in the message and further restricts the type of content that can be contained in some fields (e.g. IPAWS restricts the number of vertices in a polygon to 100). While these restrictions

create an easy environment for interoperation between many systems and vendor products, they may also limit creativity of the alert and warning vendor community. As technologies advance, a need may arise for new data elements in the CAP message which may require using a formal standards process to socialize, develop consensus, and provide configuration management of the standards interfaces. Standards processes can become lengthy and resource consuming delaying rapid deployment of new technologies..

5.1.5 Emergence of Profiles under CAP

Depending on the nature of the emergency, emergency managers may see fit to restrict the dissemination of the alert over specific service types (EAS, CMAS, NOAA Weather Radio, sirens, highway signs, etc.) The current CAP standard and the IPAWS implementation provides managers with that flexibility. Specification of particular AD channels may also be useful during tests, e.g., an emergency manager may be interested in testing CMAS only.

If an emergency manager wants to disseminate the alert over sirens, then the manager may be required to waste valuable time, essentially, in populating required fields in the alert messaging template that are irrelevant to sirens. A profile is a narrowing of the larger standard – one reason for creation is to meet practical requirements of a sub-group employing the standard. In the case of CAP, one popular profile that has emerged is the IPAWS profile, which has been largely dictated by the IPAWS-OPEN AA's objective of meeting the needs of its two biggest user groups namely EAS and CMAS.

Other CAP profiles have emerged (Canada has finalized and Australia is developing CAP profiles through the OASIS process). IPAWS and the equivalent Canadian system have developed an interface to exchange CAP messages in each other's profiles. It is possible that an industry group could creating their own profile without going through OASIS (which is not a requirement for creating profiles) which could result in competing systems that do not interoperate. However, a vendor who does so would limit their market to only users that buy and use their system end-to-end. Extensibility does not solve all the issues – in some cases one profile could mandates a data element that is optional in another, creating an interoperability problem.

One way of handling the issue of a profile-mandated element was enhancing CAP specification to enhance CAP's error message to be able to transmit "soft errors" whereby an AA or an AD can indicate to the AO (a) that their CAP message does not adhere to a specific profile required by the AD, and (b) how to rectify the CAP message.

5.1.6 Widespread CAP Adoption Including States/Local/Tribal Governments

State/local/tribal governments are major "users" of alerting systems – indeed they were the earliest customers of alerting technologies, and therefore many of them have legacy stovepipe systems that do not use the CAP data format. If the goal is to standardize the format of the alert origination message, then States having their own data formats, greatly weaken the CAP specification. Also if States do not use CAP (or the IPAWS profile of CAP), then they cannot utilize FEMA's alerting gateway, which implies that their citizens would be denied both CMAS alerts and CAP EAS alerts from those governments.

The goal of CAP is to be the one standard for alert messages – this comes at the expense of having a large number of fields. If a large number of fields needs to be populated for the message to be valid, then this can be overbearing for emergency managers (who are presumably originating the alert under duress), even with the aid of automation. This could lead to lower popularity of CAP.

5.1.7 Impact of IPAWS-OPEN on CAP Reputation

Assuming CAP is the desired data format standard for alert messages, its success may be impacted by the reputation of IPAWS-OPEN. Since CAP is most heavily used in conjunction with IPAWS Gateway, any weaknesses in IPAWS-OPEN may reflect poorly on CAP, lessening its appeal. With private sector companies creating their own alert aggregators, the perception of IPAWS may suffer. Even so, the United States Department of Defense, Canada and Australia have officially adopted CAP and are implementing alert and warning systems to receive and distribute CAP messages. The European Union and several member countries are investigating the use of CAP for exchange of alert and warning information.

IPAWS-OPEN is currently maintained by FEMA, which does not include enterprise data services as one of its core mission functions. The current implementation of IPAWS-OPEN in FEMA datacenters has some perceived weaknesses including reliability, security and scalability. Other perceived weaknesses include the process of interconnecting with it (for AOs and ADs). Perhaps moving the development and maintenance of IPAWS-OPEN to another DHS component or other government agency that has data services as a core mission and capability would help to alleviate these perceptions.

An additional weakness is the perception that FEMA-IPAWS does not rigorously enforce the CAP specification. Several AOs vendors upload sub-compliant alert messages to see if they would be accepted and transmitted by the system, and in some instances they were.

Another weakness is the uncertainty in continued FEMA funding for IPAWS-OPEN, which means less trust in IPAWS-OPEN being maintained and upgraded to the standards and service levels that would be expected in the private sector. Among desired new features are stronger middleware for handling multiple profiles and validating that a received message adheres to the requirements of individual profiles.

Although a federated architecture (see Figure 3 for an example) allows for multiple AAs, it is important that there be a federal government-connected AA. Public safety officials would not want to rely on an aggregation service with an inherently uncertain economic model, little or no oversight, and few or no contracts in effect (i.e., these third parties could discontinue service at their discretion, leaving a public warning gap).

If it is deemed beneficial to outsource the operation and maintenance of IPAWS-OPEN to one or more private-sector entities, then it can be done with heavy oversight and reporting requirements, as was the case with outsourcing wireless number portability operations to Neustar.

5.1.8 Limited Incentive to Adopt CAP

Assuming CAP is the desired standard, there may be limited incentive for vendors and emergency managers to incur the costs in equipment, inspections, and manpower to implement CAP-compliant capabilities. Even if CAP is not the desired standard, it is likely that the championed data format will experience the same phenomenon.

Some vendors of origination tools claim to be CAP compliant but are not really. (Some are compliant only with an earlier version of CAP, while other origination tools claim "compliance" but produce CAP messages with seemingly loose interpretations of the standard. Some vendors support CAP in only part of their product interface. A standard must be enforced. Even FEMA-IPAWS does not enforce the standard fully. Some vendors attempt to upload non-compliant messages to FEMA-IPAWS to see if they "stick."

5.1.9 Multimedia Alerts

Multimedia alerts by definition present the alert in multiple formats. This is beneficial as a way to mitigate the risk of one format not being understood by the AR, e.g., by people with disabilities or by non-English speakers.

Social scientists suggest that alert recipients don't often take decisive lifesaving action until the recipient receives reinforcing information. Multimedia alerts by definition present the alert in multiple formats. Thus, they are beneficial as way to personalize the alert, so that it is internalized by the recipient, information is reinforced, and the recipient is more likely to take lifesaving action. Providing alerts in multimedia formats can provide accessibility for people with disabilities and non-English speakers.

However, there are feasible alternatives to enhance public safety even when bandwidth poses limitations. For example, CMAS could conceivably broadcast the alert geo-codes to the mobile device and compare it against location based information from the device (i.e., the user's location) and/or user configurable geo-location information on the device to determine if the user should be notified of the alert. The alert geo-codes can also be used to overlay the alert area and other information from CAP messages (e.g., storm location and projected path for tornadoes) on devices with built-in maps.

Another potential alternative where available bandwidth poses limitations is to mitigate the effects of network congestion by making use of a device's built-in features to provide richer content. This would be possible where the user's device would already contain some of the reinforcing information that the user would have otherwise sought following receipt of a text-only alert.

Alerts may consist of several components including text, text for CMAS, audio-visual information, etc. Multimedia components of alerts likely have high bandwidth requirements, and may therefore not be appropriate for systems where congestion may occur. One of the advantages of a system such as Mobile EAS is that it is designed to easily handle simultaneous transmission of multimedia assets as part of its CAP-profile alerts. Mobile EAS from television broadcasters allocates relatively small amounts of spectrum (already allocated to the broadcaster) to send multimedia alerts to an unlimited number of receive devices, but this

technology has not been commercially deployed.

The multimedia bandwidth requirements are applicable to every form of transport the alert goes through i.e., Alert Originator to Alert Aggregator, Alert Aggregator to Alert Disseminator, and Alert Disseminator to Alert Recipient. Focusing on Alert Disseminators (ADs), not all dissemination transport channels (dissemination channels) can handle that requirement:

- In some cases, ADs are inherently incapable of disseminating multimedia alerts e.g., pager networks, sirens.
- In other cases the capability changes with load conditions e.g., congestion in the case of data/communication networks. Although wireless networks are obvious examples where congestion can occur, it can also happen with wired networks. It is also possible that the congestion has occurred due to people reacting to the emergency, e.g., picking up their phones as soon as they hear about the emergency. The alert itself could start this "snowball" effect. (It is for that reason that CMAS rules do not allow phone numbers or URLs in the CMAS message.) It is also possible that congestion has occurred due to reduced capacity of the network, such as if the emergency itself knocked out radio towers, fiber/copper runs, or other facilities.
- For some ADs, the technology for handling multimedia alerts in a non-crippling manner exists but is not widely deployed at present. For example, cellular providers can use a multimedia broadcast technology (referred to as MBMS) that is similar to the cell broadcast technology used for CMAS.

Most dissemination networks (e.g., TV/Radio, cellular) are not dedicated to alerts and do not have a primary mission to be an alerting network. Alerting is secondary to the mission of providing business-as-usual telecommunication/broadcasting services, even in times of disaster and emergencies.

Upgrading an AD's infrastructure to handle multimedia alerts in a manner that does not impact the primary mission of the AD likely requires an extra investment by the AD – any financial burden to the AD is a disincentive to making that investment; and the larger it is the bigger the disincentive.

It would seem appropriate for ADs to have control over the decision of whether to carry/drop high-bandwidth elements of alert over their dissemination channels to ensure that that the primary mission of the AD's infrastructure does not suffer.

5.1.10 AO/AA Need to Verify Message Dissemination

Alert Originators (AO) need to know which components of the alert were disseminated. This includes knowing whether or not the multimedia component was disseminated. That knowledge may help the AO anticipate public response and/or assess if the public has been sufficiently alerted.

It may also be helpful to the Alert Aggregator (AA) to know which components of the alert were disseminated, in order to forward that information to the AO. The Alert Disseminator (AD) would need to provide that information to the AA/AO. This creates an extra burden on the AD.

However, the act of providing feedback of similar information is already done in the case of CMAS – some CMSPs provide feedback to IPAWS-Open (although currently this feedback is only an acknowledgement that the alert was disseminated).

The burden is complicated by the fact that congestion levels vary, and therefore the ability of the AD to disseminate the multimedia component may change over time. Providing real-time status update from the AD to the AA/AO can be burdensome and costly.

5.1.11 No Clarity on Required Records

It is not clear if AAs and ADs need to (or should) maintain detailed records (e.g., logs, operational measurements) on disseminated alerts, containing whatever information is available to them. Such records may be needed for training, retrospective analysis, and/or legal purposes. For example, the FCC may want to study these records to advise/control AOs who over-alert.

Should such records be required, it is not clear what level of detail would be required. For example, do ADs need to have a second-by-second account of which multimedia components were disseminated? The level-of-detail requirement could be overly burdensome and costly for AAs/ADs. In the case of CMSPs, they may decide to disable all multimedia communication from/to mobile devices (e.g., if citizens want to get local TV streams about the emergency event) – should such a decision also be included in the alert record? The more information in the alert record, the more burdensome it will be to ADs.

In addition it would be unclear where that record would be kept/stored and for how long, and also what protocol would be used to govern how/when/to whom AAs/ADs provide those records.

5.2 Platforms

5.2.1 Alert-Receiving Communication Devices

5.2.1.1 Introduction

The scope of this discussion will be limited to devices that require explicit user action to opt out of receiving alerts. In other words, this analysis does not consider “opt-in” alert services where the user could actively subscribe to alerts from a variety of web-enabled devices. Any device with a Broadband or wireless Internet connection should, at some point in the future, receive emergency alerts without requiring user action.

5.2.1.2 Common Characteristics of Next Generation Communication Devices

Ideally, from an ergonomic/functional standpoint, the devices need to have a graphic display with storage, to allow for user replay of the messages at a later time, with clear indication of the alert validity period. An application to display such messages would be appropriate for device management of emergency alerts, but an embedded service could also suffice. The device must also provide an attention-grabbing method to alert the user or resident, such as an audible tone, vibratory action, or flashing indicator. Wherever possible, the ergonomic requirements defined for mobile devices in the CMAS Mobile Device Behavior Specification J-STD-100, which was jointly developed by the Alliance for Telecommunications Industry Solutions (“ATIS”) and the

Telecommunications Industry Association ("TIA") and defines a common set of requirements for how CMAS-capable devices will behave upon receipt of a commercial mobile alert, should be considered as a baseline specification for these new, currently unsupported, devices.

Additionally, the devices should allow for user configuration of alert types to be received, similar to the procedures and data types discussed in Section 10 of J-STD-100. The devices should support the ability to receive geo-targeted alerts. The details of the geo-targeting mechanism are network dependent, and do NOT necessarily imply any location capability for the device itself. The device does not need to acknowledge any alerts.

Examples of devices to which emergency alerts can be extended include desktop PCs, laptop PCs, and Wi-Fi tablets. All of these devices have rich operating systems and application development environments. Devices with limited visual output displays should also be considered. These could be devices such as home alarms, a Blu-Ray players, set-top boxes, etc., provided that they have constant connectivity to an AD or AA through some access and transport technology. Some of these devices normally operate in "Always On" mode (unlike a PC or TV set), and thus may be able to alert the user at any time. One of the features being considered for these devices by designers is a "wake up" capability, to justify sending alerts to devices that may be in standby or sleep mode.

5.2.2 Aggregation Systems

5.2.2.1 Introduction

This is essentially a question around having one central alert aggregator vs. multiple entities performing the alert aggregation functionality (see Appendix C). Should it be through one source, as it has been traditionally, or should there be multiple ways an Alert Originator sends out alerts? For example, can Google CRT's aggregator and other potential Alert Aggregators receive the same alert an Alert Originator sends to FEMA's IPAWS-OPEN and in turn make it available to Alert Disseminators, including the AA itself acting as an AD and sending the alert out to its end-users?

5.2.2.2 Advantages of Single Aggregator

For nationwide coverage, the single aggregator is what is currently in place (there are reportedly several state-level aggregators in use) in the form of IPAWS-OPEN, and for the most part seems to be functioning at a high level and satisfying the needs of all players involved. Having a single point of control with a technology is rare and something that should be retained unless there is an overwhelming case made that progress is being held back.

Given the importance and the impact of how the public responds to emergency alerts, it is beneficial to have a trusted single source for alerts, which helps manage the distribution of information and prevent incorrect use (or misuse) of the alerting system. The single source for alerts also provides some level of reduction in liability to private-sector providers of alert dissemination networks and services.

Single point of control allows for a technology to be directed in an open standards-based universe much more easily and provides a framework around which to encourage

interoperability between vendors and alert and warning disseminators. It obviates the need for a governmental body/program to oversee and manage multiple Alert Aggregators including performing the following tasks:

- Certification
- Auditing
- Central directory for lookups
- Enforcement of service level requirements could be difficult

While having multiple aggregators offers systematic redundancy, it also creates multiple targets for cyber-attacks, making the defense of the overall architecture more difficult. In addition, having multiple aggregators may add complexity to the dissemination (e.g., coordination to prevent multiple copies of the same alert over the same dissemination channel, possibly resulting in missed alerts.

5.2.2.3 Disadvantages of Single Aggregator

Although the current configuration is operational, no effort has been made to define what is not working today or what additional capabilities are lacking in the current setup.

With the system under a single entity's control, the public safety alerting technologies are subject to being held back by any bureaucracy present within that single entity. The single aggregator may become too focused on traditional communication mediums while ignoring cutting-edge technologies used by younger generations without proportionate/adequate representation in the standards bodies.

If the single aggregator is physically a single server, then it will be an attractive target for cyber-attacks that may render it inoperative. Even if the alert aggregator is physically implemented as a network of redundant, load-balanced, mirrored servers, it will still present itself as a single system to target for an attack.

If a technical failure (e.g., software bug) brings down the single aggregator (regardless if physically a single server or a network of servers), then the overall architecture will experience near-complete failure, as opposed to the partial degradation that would occur if multiple aggregators were to be used.

A single AA implies a monopolistic provider of the AA service, which will not necessarily respond the needs of AOs and ADs with the desired urgency. A single AA will have to handle the entire load of certain labor and/or process intensive operations such as identity verification of AOs. Having multiple AAs, especially if organized as a hierarchy mirroring local-state-federal jurisdictional hierarchy, would result in distribution the load of such operations. In addition, having a single AA likely prohibits the possibility of commercial for-profit Alert Aggregators, which may be better, faster, and more efficient for ADs and AOs in certain respects.

5.3 Implementing New Dissemination Technologies on a National Alert Platform

5.3.1 Introduction

This topic deals with the role that the FCC can play in easily and effectively bringing in new AD technologies into the then-existing national alerting platform. Should there be an established national alerting architecture serving next-generation alerting[3] in the United States, it is likely that the current FEMA Integrated Public Alert and Warning System (IPAWS) architecture will be the basis of/template for it. Currently, FEMA IPAWS aggregator supports EAS dissemination via-TV/Radio/cable/satellite broadcasting, the cellular broadcast (CMAS) and NOAA weather radio dissemination channels. These alert dissemination technologies have been implemented via a mixture of legislation, voluntary participation, funded and unfunded mandates and FCC rulemaking to require adherence with an outcome consistent with the IPAWS platform. Placeholders for Broadband, Wi-Fi, social networking and other yet-to-be defined alert dissemination technologies are indicated in IPAWS's general purpose architecture diagram. IPAWS's goal is to incorporate as many dissemination capabilities as possible in order to provide maximum coverage for the US public and connection for the US citizen to timely and accurate alert and warning information.

Given the presence and future plans of IPAWS, it is not clear that the FCC is the only federal agency responsible for facilitating new alert dissemination technologies. It is possible that such an initiative needs to be conducted jointly by the FCC and FEMA, potentially with involvement by the National Weather Service and the United States Geological Survey (USGS).

5.3.2 Objective

Assuming the FEMA IPAWS architecture to be the national alerting architecture, the objective of this section is to identify mechanisms and challenges for adding new dissemination outlets to the alert framework. This includes existing dissemination technologies that have not yet been incorporated into the FEMA IPAWS platform, as well future alert dissemination technologies that have yet to be invented/implemented/deployed.

5.3.3 Observations about Existing IPAWS-Supported Dissemination Technologies

The alert aggregator was defined and is operated by FEMA. Accordingly, FEMA dictates the rules of operation and connectivity to which ADs must adhere. The dictation of operation/connectivity of rules by a single entity has resulted in high degree of clarity about said rules for ADs.

The FCC has reinforced FEMA's efforts by writing rules that are consistent with FEMA's rules, e.g., CAP protocol requirement, behavior of broadcast technologies on the alerting network edge, etc. Alert disseminators operate independently. The standards-setting process has been developed along industry and technology lines. There have been few if any cross-industry or cross-technology platforms. Industry finances the dissemination of alerts to the public. Currently, there are no mechanisms for quantifying and measuring the success and societal benefit of an alerting technology (either per occurrence or in general).

[3] In this context, the term next-generation alerting does not refer to futuristic alert dissemination methods. Rather it refers to the process, system and infrastructure through which the US public will receive emergency alert in the future.

5.3.4 Introducing New Alert Dissemination Technologies to the Public

Government pays for certain steps in the alerting activity chain (e.g., FEMA finances alert aggregation; federal, state, and local government finances alert origination). However, in many instances, citizens are still expected to purchase devices and services for receiving such alerts. In most cases, such devices are purchased primarily for non-alerting purposes e.g., TV/Radio, smartphones. In other cases, these devices are purchases specifically for alerting purposes e.g., NOAA weather radio.

One example of an exception would be the use of online advertising technology for alerting, because it can be considered as already integrated into legacy devices such as an aged desktop computer with Internet browser as well newer mobile devices which incorporate online advertising.

Traditionally, the introduction and widespread deployment of a new alert dissemination technology to the public has been more event-driven (i.e., in the aftermath of an event/incident) than market-driven. For example, there was a significant increase in college-campus SMS alerting in the aftermath of the 2006 Virginia Tech campus shooting.

Whether event-driven or market-driven, many AD technologies introduced in the last few years are entrepreneurial or for-profit e.g., SMS alerts, ETN, certain smartphone apps. However, not all society-benefiting AD technologies will emerge based on entrepreneurial basis – in some cases governmental intervention is required/needed either via regulation (e.g., nationwide EAS) or via encouragement and facilitation (e.g., CMAS).

Going forward, the existence of a federated architecture (IPAWS-OPEN architecture is at least one example) will lower the barriers-to-entry for new alert dissemination technologies, for at least two reasons:

- Vendors of said new technologies need not invest in building components for the entire alert activity chain.
- Vendors of said new technologies would not be easily blocked out by entrenched vendors of legacy stovepipe systems, whose existing closed alert-origination tools leave little to no "shelf space" for said new-technology vendors' alert-origination tools.

5.4 Adherence to Four Components of Digital Security

The four components of digital security are authentication, authorization, integrity and privacy. This topic also includes (a) investigating the process for authorizing alert originators and (b) how to ensure that a received alert is real. There are several paths messages take, all of which have security concerns:

- The message originator sends messages to some kind of message aggregator (like IPAWS-OPEN). The message aggregator sends messages to various Alert Disseminators (such as a wireless network operator). The AD delivers the alert message to citizens.

- In each step, there could be intermediaries who provide "fan-in"/"fan-out" services to

keep the number of entities a given element needs to handle to a reasonable number. For example, a network operator may have 2 or 3 levels of distribution to get a message to the consumer.

Each of these paths needs security with at least authentication, integrity and privacy, and where messages cross administrative boundaries, authorization decisions must be made.

IPAWS has implemented authentication and protection of message integrity using digital signatures. IPAWS will only process alert messages that are digitally signed by the AO with a certificate issued to the public safety organization by FEMA during the user registration process. The digital certificate of the AO is maintained throughout the IPAWS distribution of the alert to the distribution channels to ensure that the AO's message integrity is maintained. Both NOAA and participating CMAS wireless carriers validated message certificates before any alert is distributed through their networks. FEMA strongly encourages all EAS participants to also validate an alerts certificate before broadcasting the alert message.

5.5 User Opt-In/Opt-Out Control

In most circumstances, the targets of an alert are defined by geospatial relationships (affected area). However, there are many circumstances where this is not sufficient. One is where the target has no way to determine where it is, and geo-targeting would not work except on a predetermined, relatively coarse level. Another example is where there is a desire for one entity to get alerts geo-targeted to another entity. For example, a parent may wish to receive alerts originally targeted to their child. There are also classes of alerts that should not be received by an entity even if they are in the geo-targeted area. These may be low priority alerts. In all of these cases, there is an explicit opt-in action taken by the target in advance of the alert.

6 Social Media Alerting

6.1 Variety of Social Media Categories

In the context of present-day social media (SM) alerting, most discussions revolve around two particular Social Media Providers (SMPs), namely Facebook and Twitter. However, it is important to note the world of SMPs is bigger than Facebook and Twitter and involves services beyond social networking and micro-blogging.

One description of social media services that seems apt is the one used by Wikipedia, namely: "Social Media includes web-based and mobile based technologies which are used to turn communication into interactive dialogue between organizations, communities, and individuals."

It is beyond the scope of WG2's work to conduct a survey and an analysis of the complex SMP market. However, it is important to bring attention to the relatively large number of existing SMPs and the existence of different categories of SMPs. One approach for elucidating these different categories of SMPs is provided in the table below. This identifies eight categories and is not meant to be an exhaustive list of categories or SMPs:

No.	Category	Description	Examples Known Principally for that Category[4]
1	Social Networking	Interact by adding friends, commenting on profiles, joining groups and having discussions	Facebook, Google+, MySpace, Foursquare, Hi5, Yahoo! Groups
2	Blogs / Microblogs	Interact by exchanging small elements of content such as short sentences, individual images, or video links with followers.	Twitter, Tumblr
3	Content Communities	Interact by sharing photos or videos and commenting on user submissions.	YouTube, Pinterest
4	Virtual Game Worlds	Interact within an online community that takes the form of a computer-based simulated environment through which users can interact with one another and use and create objects. Users typically take the form of avatars visible to others. Users are usually required to follow strict rules that govern their behavior, and often are not allowed to engage in economic activities.	World of Warcraft, EverQuest
5	Virtual Social Worlds	Interact within an online community that takes the form of a computer-based simulated environment through which users can interact with one another and use and create objects. Users typically take the form of avatars visible to others. Users do not have any restrictions on the way avatars can behave or interact, including the possibility of conducting business/commerce with other users.	Second Life, Twinity
6	Collaborative Projects	Interact by adding content and editing existing content.	Wikipedia
7	Social Bookmarking	Interact by tagging websites and searching through websites bookmarked by other people.	Del.icio.us, Blinklist, Simpy
8	Social News	Interact by voting for articles and commenting on them.	Digg, Propeller, Reddit

Table 5 – Categories of Social Media Activities

It is important to note that while Facebook and Twitter are the most dominant forms of using social media for alerting today, it is possible that emergency managers will find in the future other forms of social media services that are equally or more effective in disseminating alerts.

[4] Many Social Media Providers offer services that span multiple categories. For example, while Google+ is known primarily as a social networking service it offers capabilities such as embedded YouTube feeds and collaborative document creation. Therefore arguably Google+ also belongs in the Content Communities and the Collaborative Projects categories. However, it is known primarily as a Social Networking service.

6.1.1 Terminology

The terminology in this section is an extension of the terms already established in the previous section, namely: Alert Originator (AO), Alert Aggregator (AA), and Alert Disseminator (AD). Different social media providers have different names for similar if not equivalent entities. For example, if someone establishes a social networking connection to another person on Facebook, then the former is referred to as a *friend* of the latter. In the case of Google+, the former is referred to as a *member of a circle* belonging to the latter. In the case of Twitter, the former is referred to as a *follower* of the latter.

In order to facilitate the subsequent analysis, Working Group 2 uses the following definitions for concepts/entities that may be common across different social media providers, but have different names:

- **Alerting Account:** A social media account (e.g., on Facebook, Twitter, and/or Google+) that is set up by a public safety official for the purpose of alerting the public in their jurisdiction.
- **Subscriber:** Subscriber refers to a social media user who has signed up to receive alerts from the *alerting account*. For example:
  - In the case of Facebook, it would be citizens who signed up as *friends* of the emergency manager's Facebook *alerting account*.
  - In the case of Twitter, it would be citizens who signed up as *followers* of the emergency manager's Twitter *alerting account*.
  - In the case of Google+, it would be citizens who signed up as a member of a circle within the emergency manager's *alerting account*.

6.1.2 Other Efforts Related to Social Media Alerting

The use of social media in emergency management has received significant attention, both within and outside the public safety community. Here are some examples:

1. The Alerts and Warnings using Social Media (AWSM) Program within the U.S. Department of Homeland Security, Science and Technology Directorate (DHS S&T). Among other activities, the AWSM program sponsored a two-day workshop entitled "Alerts and Warnings Using Social Media: Current Knowledge and Research Needs: A Workshop" on February 28-29, 2012 at the Beckman Center, Huntington Room, Irvine, CA. The workshop was organized by The National Academies. The full report on the workshop is available at http://www.nap.edu/catalog.php?record_id=15853.
2. A Congressional Research Service report entitled "Social Media and Disasters: Current Uses, Future Options, and Policy Considerations" (authored by Bruce R. Lindsay); published on September 6, 2011.
3. Social Media topic within AWARE Forum (http://www.awareforum.org/category/social-media/) – AWARE is an independent forum that brings together thought leaders and practitioners in the public safety and emergency management fields to share ideas, discuss key insights, and learn about best practices in emergency alerts and warnings. Sponsored by SRA International's Strategy and Performance Group the purpose of AWARE is to offer a source for information and rich discussion for SRA's clients, potential clients, and alerts and warnings stakeholders.

4. A Department of Energy report entitled "Social Networking for Emergency Management and Public Safety" (authored by AM Lesperance, MA Godinez, and JR Olson); published in August 2010.

In addition, a relevant example of the use of Social Media in Emergency Management by the American Red Cross is provided in detail in Appendix E.

6.1.3 Intervention of Social Media Providers in Delivering the Social Media Alerts

The only way of using social media alerting *today* entails emergency managers setting up *alerting accounts* and trying to have as many *subscribers* as possible. In other words, the *alerting accounts* are regular social media accounts that happen to be owned and operated by emergency managers.

Today, Facebook and Twitter are the dominant social media platforms used for alerting. When an incident occurs, the emergency manager posts a message on the *alerting account* for their *subscribers* to view. This is no different from an average social media user posting a message for their friends/followers/circle members to view.

In the future, it is possible for social media providers to treat emergency alerts as an exceptional category of messages/posts and to intervene in order to ensure that the emergency alert message is delivered to the intended audience with greater efficacy. This may include ensuring the fastest possible delivery or higher priority in delivery, visual highlighting of the message to increase its attention grabbing potential, etc.

Intervention by social media providers may also include plugging into an Alert Gateway (e.g., FEMAs IPAWS-OPEN), and upon detecting a new alert on the gateway, inserting the alert into the Social Media User's content (e.g., Facebook wall), potentially with geo-targeting as discussed in section 6.1.9.

6.1.4 Social Media Alerting Opportunities

6.1.4.1 Training Emergency Managers

There should be a training program for emergency managers on the use of social media for issuing alerts and warnings to the public. Preferably this training program should be approved by an authoritative source, and publicized so that it becomes widely known as the go-to training program for emergency managers.

6.1.4.2 Training Sources

Today, there are several providers that offer training in social media alerting including:

- FEMA: Recently began offering IS-42 Social Media in Emergency Management (https://training.fema.gov/EMIWeb/IS/is42.asp)

- International Association of Emergency Managers: Typically have training seminars at their conferences.

- National Disaster Preparedness Training Center at the University of Hawaii: Offers a touring course entitled "Social Media for Natural Disaster Response and Recovery" (see https://ndptc.hawaii.edu/training/catalog/8).

Existing training providers can give valuable input on the creation of a comprehensive training program based on their lessons-learned. Existing training courses can be converted into non-overlapping modules within a comprehensive training program, such that existing training providers have an incentive to contribute constructively to the creation of the comprehensive go-to training program.

The comprehensive program may potentially be a mix of for-fee and free training modules.

6.1.4.3 Social Media's Continuous Evolution

Social media is continuously changing. Change may be technological in nature, whereby an existing social media provider adds new features/technologies to its offering. Change may also be in the form of the arrival of a new popular social media service.

6.1.4.4 Emergency Managers' Challenges

Emergency managers are short on time and financial resources. They cannot be expected to attend multi-day training courses.

Differences in jurisdiction and local laws and procedures are also a challenge. According to a recent finding reported during a program titled "Alerts and Warnings Using Social Media" conducted by the Science and Technology Directorate of the U.S. Department of Homeland Security, one-size solution approach does not fit all – different communities or jurisdictions have different needs, technology comfort levels, expectations, etc.

Another challenge comes in the form of common barriers-to-adoption that are experienced or interposed by Emergency Managers. Academic research points to several barriers to adoption of social media alerting by emergency managers including:

- Fear of a new technology.
- Lack of internal policies governing the use of social media alerting.
- Lack of knowledge on how to use social media for alerts and warnings.
- Public expectation of being able to communicate directly with public safety officials over *alerting accounts*.

6.1.5 Promoting & Funding of Innovative Tools that Enhance Social Media Alerting

6.1.5.1 Publicizing Strategic Vision

The FCC should encourage a unified strategic vision for value-added IT/Internet tools that enhance the efficacy of social media alerting. In order for entrepreneurs, open-source software developers, and other federal agencies to reinforce that strategic vision, it is important that the vision be made available to the public in a clear and unambiguous fashion.

6.1.5.2 Support of the Open-Source Developer Community

The open-source developer community has long provided freeware to computer users and software developers. It is not uncommon for such freeware to be a substitute for commercial software. The open-source developer community may provide free or low-cost substitute IT/Internet tools for budget-limited Emergency Managers as well as IT/Internet tools with new capabilities that address needs outlined in the strategic vision.

6.1.5.3 Limited Governmental R&D Funding

Some IT/Internet tools may be developed by entrepreneurs who are able to identify a profitable business model. However, commercial profitability in the field of alerts and warnings has traditionally been difficult. Tools may not be developed by the private sector, because such development may not be anticipated to be profitable, or as being likely to achieve profitability only after a long time – both cases are typically avoided by venture-capital funding. Government R&D funding is generally required to support product development in such cases.

The DHS Science and Technology Directorate and the FCC have limited budgets for R&D of alerting technologies. Other federal agencies concerned with public safety may be able to provide such funding also.

6.1.6 Scope of Social Media Alerting

6.1.6.1 Coupling Social Media Alerting with Citizen Responses

One unique aspect about social media alerting is that issuing an alert automatically and immediately sets up a two-way communication with citizens over the alert dissemination medium – other dissemination channels that arguably exhibit this aspect are Emergency Telephone Notification (ETN) e.g., Reverse 911(TM), and Email.

Issuing an alert over social media typically results in a large number of responsive incoming messages from citizens. The more subscribers an emergency manager has, the more responsive messages the manager is likely to receive.

According a survey conducted by the American Red Cross (see http://www.redcross.org/news/press-release/More-Americans-Using-Mobile-Apps-in-Emergencies), "Three out of four Americans (76 percent) expect help in less than three hours of posting a request on social media, up from 68 percent last year. Forty percent of those surveyed said they would use social tools to tell others they are safe, up from 24 percent last year." Whether or not emergency managers have the necessary resources to respond to citizens over social media, there is a public expectation that they will.

The American Red Cross study demonstrates the general public's increasing engagement and reliance on social media for emergency related communication.

6.1.6.2 Restricting Two-way Communications

It may be beneficial to restrict two-way communication on *alerting accounts* so that only

emergency managers can post messages on them, thus controlling the content and limiting the volume incoming messages traffic. However, such a limitation may hurt the ability of emergency managers to attract subscribers.

Additionally, such a limitation prevents citizens from posting legitimate call-for-assistance messages on *alerting accounts*. The net benefit/cost of restricting two-way communication is not clear to the Working Group.

6.1.7 Hidden Cost of Social Media Alerting

Although alerts are issued via social media without charging the recipients, there are significant costs attached to the use of this medium. Human resources are needed to monitor, "nurture", and grow subscriber-base of the *alerting accounts* during business-as-usual periods.

During emergency periods when incoming messages will normally spike, there is the greatest demand on these human resources. The purchase of, maintenance of, and user-training for systems aimed at aiding the emergency manager with using social media add to the cost – even freeware requires maintenance and training.

6.1.8 Understanding Public Response

The public is unaccustomed to social media alerting relative to traditional alerting channels. Even with the long established EAS, monthly tests help educate the public about what to expect if an alert is actually sent out.

Given the ease of person-to-crowd communication over social media, a new phenomenon may emerge whereby citizens take it upon themselves to issue emergency alerts to their communities directly.

This phenomenon is perhaps facilitated by the perception (or reality) of emergency managers being behind the curve on the use of social media. Some researchers are calling not only for the acceptance of the phenomenon of "user-generated" alerts, but also for embracing it. Even though there is value in sourcing information from citizens via social media, arguably, delegating emergency notification to non-professional citizens can have negative consequences.

6.1.9 Geo-Targeting Social Media Alerting

Social Media Alerting has no inherent geo-targeting capability. At the same time, there is value in sourcing information from citizens via social media. Even if we assume self-selective geo-targeting by virtue of signing up with the local Emergency Manager, unaffected people may still receive the alert, contributing to a cry-wolf effect, which in turn increases chances of tuning out such alerts in the long run. At the same time, some people who are affected by the incident may not receive the alert, putting them in danger.

IP-Location lookup is often cited as a method for geo-targeting; however it is not reliable enough for emergency alerting. (Note: It will also require SMP intervention). The issue of geo-targeting for social media alerts is almost equivalent to the issue of geo-targeting for Broadband alerting. In the case of access without the use of GPS (i.e., web-browsers on traditional

computers), the intervention of the SMP is necessary and that of the ISP may be needed. In the case of GPS-available access (i.e., custom mobile apps on smartphones), the intervention of the ISP is necessary.

6.1.10 Social Media Alerting and the Subscriber

Citizens must opt-in to receive social media alerts. A different approach would be to have ISPs inject the alert into the network traffic carrying the social media data. However, such "injection" may be deemed to be offensive or too aggressive, and it may lessen inherent trust in the message.

One advantage of subscription is that once a citizen has subscribed, the person would not be surprised if an alert message is received – immediately there is more trust in that information.

In the age of the Internet and social media, the public expects information to be delivered instantaneously. It is sometimes argued that the public would value speed over accuracy, whereby information comes out quickly and is updated later, rather than temporarily delaying its transmission pending verification.

In the case of social media, the emergency manager is in competition with other sources that may send out their version of the alert first, which could lessen the audience for the emergency manager's message.

The FCC should examine whether legacy procedures for issuing emergency alerts are optimal in all cases in the age of social media, especially in terms of speed of issuance.

6.1.10.1 Crowd-to-Crowd Propagation

Crowd-to-crowd propagation of alerts is inevitable but uncontrollable. Inaccurate information can bleed into the content as it is being forwarded. Erroneous information can cause public reaction that aggravates the situation.

One goal is to design alert messages to spread as efficiently as possible, with as little mutation as possible. Some individuals or organizations might intentionally provide inaccurate information to confuse, disrupt, or otherwise thwart response efforts.

For example, a secondary attack after an initial attack can be planned to kill and injure first responders, by using social media to notify officials of a false hazard or threat that requires a response, especially in the immediate aftermath of the first attack.

6.1.10.2 Alerting Accounts

Other trusted sources can be allowed to put helpful information on the alerting account, e.g., fire department. Establishing the trustworthiness of a source is necessary, and a cooperative agreement between agencies is one way to establish trust prior to an emergency.

If there is no clear process for determining the trustworthiness of the third-party source, then there is a risk of malicious abuse of trust by those placing misinformation for purpose of

creating a panic.

Firsthand accounts from citizens can be posted on the alerting account. However, verifying the accuracy of information from citizens can be difficult.

6.1.10.3 Limited by Available Data

Public response to SM alerting can be better understood and predicted via social sciences research. A standard way of conducting social science research is by looking at population data to determine societal macro-behavior. Data related to the public response to social media alerting may be difficult to attain.

Some responses are not easy to measure via well-defined data. Some SMPs, who probably own the data, may not feel comfortable disclosing whatever data they have and making it publicly available.

At the same time, legitimate privacy concerns exist about the potential for the collection, retention, and data mining of personal information by governments.

A message on Twitter or Facebook is not limited to the 90 characters of the CMAS protocol – however, it is still important to know what to put in that message and in what order to convey the information as effectively as possible to citizens

Prioritization of actionable life-saving information is important. This may be particularly true for individuals with disabilities.

6.1.10.4 SM was not Built for Alerts

Unlike most of the other alert dissemination technologies, social media was not built to be optimized for sending emergency alerts. Yet, as social media has become a dominant communication force in today's society, the prospect of maximizing or at least enhancing the potential of social media for alerting is very appealing.

Social media has given rise to a variety of non-authoritative yet credible sources for alerts, such as the Red Cross.

One advantage of this phenomenon is that citizens can get confirmation of alert information from multiple sources, which adds creditability to the information and increases the sense of urgency to respond to it.

A disadvantage of this phenomenon is that traditional government emergency managers now must compete with multiple non-government sources, including loss of control over information being sent out.

6.1.10.5 Elite Users

Elite users are social media account holders who in their own right have a large number of subscribers. To the extent that such users become active in the post-alert conversation using

social media, then they would be in position to influence public response.

The social media activity of elite users must be taken into consideration by the emergency manager, as it has the potential both of being leveraged by the emergency manager to reinforce the desired public response and of complicating the ability of the emergency manager to shape the public response in a desired manner.

6.1.11 Media Congestion

Social media alerting may trigger a sudden flurry of Internet traffic. The surge in Internet traffic may result in significant congestion of the Internet, particularly the wireless/cellular component of it. In an extreme case, the surge in Internet traffic may bring down the network completely – again especially in the case of wireless/cellular Internet. This outcome does not appear to have been experienced to-date; however as more emergency managers use *alerting accounts*, and *alerting accounts* attract more subscribers, this effect may eventually be experienced.

6.2 Social Media Alerting and the Access and Functional Needs Community

There are several groups of people with disabilities (PD) or other unavoidable functional limitations. Prominent among them are the deaf and hard of hearing (DHH), visually impaired and blind, cognitively disabled, motor skills limited and the aging.

Even within the same group, there can be several subgroups. In the case of the DHH group, there are those who have complete loss of hearing since birth, those who lost hearing at some point in their lives, and those who are partially deaf. There are similar subgroups within the group of visually impaired and blind people.

There also are communities with multiple disabilities, such as the deaf-blind. Each PD group may have certain needs that are unique to it.

6.2.1 Existing Technologies

In general, social media is consumed via computers and smartphones. Social media accessibility challenges for the PD community form a subset of general computer/smartphone accessibility (CSA) challenges. Providing alerts in multiple formats (i.e., text, graphics, video, and audio) generally improves the accessibility of alerts to people with disabilities. Social media services could leverage unique ring tones and vibration cadences for different types of hazard messages.

The greater challenge is not with the development of technological solutions, but the cost of these solutions. For example, one off-the-shelf solution that converts a text message into voice and voice into brail costs in excess of $5,000, making it inaccessible to nearly the entire community that needs it.

6.2.2 Diverse Multimedia Content is Important

Multimedia content refers to having different types of content including text, audio, and video. Multimedia content can be more diverse by having even more communication formats.

In the case of text, there can be simple text (e.g., for cognitively disabled persons and for some deaf people who have difficulty with reading) and complex text (for others who can benefit from additional information).

In the case of video, it can contain text-based captioning (possibly with simple vs. advanced language options in multiple languages) and signing.

Both sign language and captions are critical for the DHH community. Neither option by itself meets the accessibility needs of every member of this diverse community.

6.2.3 Speed of Misinformation

Certain disabilities may impede the ability to process the content of a message. Misunderstanding of information may be compounded when a person virally forwards the information after adding misinformed commentary.

Expressing the information in multiple formats within the alert message limits the probability of initial misunderstanding, and allows a second recipient to catch inconsistencies, and at least think twice before forwarding the information further. This is a form of diversification that combats the risk of confusion.

6.2.4 DHH Community More Reliant on Social Media for Emergency Information than General Public

The DHH disability impedes the ability to communicate with others. According to leading advocates for the DHH community, social media can be an effective means for overcoming such impediments, and can provide an alternate way of obtaining emergency information. It is therefore imperative to send alerts over social media for the benefit of members of the DHH community. Use of simplified text in the alert message is preferred.

6.3 Enhancement of Social Media Alerting via other Internet/IT Tools

6.3.1 Video Uploads

First-hand account video (from citizens or in-the-field public safety officials) can be uploaded to or referenced in *alerting accounts*. Video can be beneficial to (command-and-control) public safety officials for whom situational awareness may be increased. Video material can be beneficial to citizens in terms of gaining additional understanding about the emergency and acts to reinforcing information about the hazard which may encourage the citizen to take lifesaving action. YouTube has become the de facto repository for digital videos, and it is quite common for social media messages to contain links to YouTube videos.

Emergency managers may be able to facilitate uploading videos or posting links on their *alerting accounts* via social media apps. Emergency managers may also be able to facilitate uploading videos or posting links on their *alerting accounts* by configuring them to be receptive to commonly-used off-the-shelf tools for uploading videos and/or posting links.

6.3.2 Multiple Accounts

Multiplicity of *alerting accounts* (on different social media platforms) is preferred. Collectively, they reinforce each other and multiply the reach of the alert message. They also reinforce the credibility of the alert message, as the citizen is in a position to receive it on multiple social media channels.

In addition to sending emergency alerts over Facebook, Twitter, and perhaps increasingly Google+, some emergency managers have taken to sending them on other social media sites such as: YouTube, Meetup, USTREAM TV, Storify and blogtalkradio.

A significant challenge with having multiple social media accounts is that each requires logging in and posting (in addition to other interfaces for other alerting technologies). There are existing open-source tools that allow effectively managing multiple social media accounts from a single dashboard interface that includes posting a message once to all accounts simultaneously. Examples include HootSuite, TweetDeck, and Seesmic.

Additionally, alert origination tools (i.e., software applications) are increasingly tending towards a one-interface approach that automatically originates the alert for multiple dissemination channels (social media, SMS, Email, etc.). Tools that can help the emergency manager automatically send out the alert on all their social media *alerting accounts* via a single activation process would be very helpful.

6.3.3 Large Volume of Follow-up Messaging After a Social Media Alert

Emergency managers using social media for alerting want to have as many of their citizens as possible become subscribers. One unique aspect about social media alerting is that issuing an alert automatically sets up a two-way communication with citizens.

Citizens may use the two-way communication for calls-for-assistance or for requesting lifesaving directives and information at the onset of an incident, or during an incident, that could help under-prepared citizens. Citizens may use the two-way communication to provide first-hand account of situational developments that can improve the emergency manager's damage assessment and situational awareness.

Issuing an alert over social media typically results in a large number of incoming messages from citizens, and the more subscribers an emergency manager has, the more responsive messages can be expected from those subscribers. Emergency managers may observe a responsibility to respond to these messages.

IT tools (including natural language processing tools) can help emergency managers automate responses to certain incoming messages and highlight those that require manual response.

6.3.4 Prioritizing Incoming Messages

Related to the large volume of incoming messages, it may be more efficient and beneficial not to handle messages on a first-come-first-serve basis, but to prioritize those messages based on urgency, relevance, etc. Again, IT tools (including natural language processing tools) can help automatically prioritize incoming messages and present them to the emergency manager in a

specified order of highest to lowest priority.

6.3.5 Post Incident Reporting

Post-Incident reports on the performance of the alert can help make technology and process improvements for future uses of social media alerting.

Examples of performance metrics include: the number of citizens who received the alert over social media; the number of citizens who requested 911-like assistance; the number of citizens who posted response messages; the number of citizens who appropriately evacuated or sought shelter as a result of social media alerting.

Performance measurements for this dissemination channel will create data that can be analyzed post-incident to help understand how to better use this channel.

6.3.6 Other Tools

Geographic visualization tools can illustrate trends and common discussion points in incoming messages on digital maps, based on location, which in turn can help emergency managers detect patterns more easily than parsing through messages. SMP's assistance in providing location information (or estimates thereof) would be helpful for such geographic visualization tools.

Context analysis tools can detect buzzing topics early on, which can bring an important issue to the emergency manager more quickly.

As previously noted, social media sites are not optimized for presenting emergency related information. Therefore, it may be helpful to have a link to a dedicated landing webpage in the body of a SM alert message. Dedicated webpages can be designed specifically to convey emergency information and provide useful tools (e.g., translation buttons). This includes (links to) maps, links to YouTube, etc. Having a landing webpage associated with each alert allows (A) the presentation of the emergency related information using the most impactful web design known, and (B) the provision of information to the public about the emergency incident in a form that the public can trust to be free from commentary and annotation by other users as they copy, paste, and forward messages.

The *alerting account* ideally should automatically post any applicable emergency alerts sent to an AA (e.g., if the geo-targeting includes the *alerting account's* jurisdiction). This would require having an open channel between the *alerting account* and the Alert Aggregator.

If a social media alert goes out on a State emergency manager's *alerting account*, it will not automatically appear on a local emergency manager's *alerting account*. It would be helpful if *alerting accounts* immediately and automatically reposted alert messages from *alerting accounts* corresponding to subsumed jurisdictions.

As more emergency managers use social media for alerting, and more citizens receive alerts via social media, the potential for improving the efficacy and practicality of social media alerting through supporting technological tools will also increase.

Evidence of the value of supporting software tools anecdotally evident via the example of the American Red Cross' Digital Operations Center (Appendix E).

The next step would be to act on some or all of the individual areas highlighted above as a first step towards developing a strategic vision for the enhancements of social media via supporting software tools.

6.4 Involvement of SMPs in WG2

Despite substantial efforts at outreach and recruiting from the Working Group, social media providers chose to play a very limited role in the Working Group's activities. No social media company authorized any of its employees to seek to become a member of WG2. A representative of one social media provider participated in a number of WG2's conference calls, and representatives of two more social media providers made presentations by phone to a face-to-face meeting of the Working Group. In these contacts, the providers noted their recognition of the important roles that their organizations might play in alerting the public. They disclosed that they have been approached by other entities regarding alerting issues. They spoke of the existence of on-going internal initiatives and plans for new services aimed at supporting emergency alerting over social media without revealing the details of those initiatives or services.

WG2 interpreted the perceived lack of interest by SMPs in supporting social media alerting as possibly being caused by one or more of the following concerns:

- Extra economic cost to SMPs without an obvious source of revenues for the service rendered.
- Necessity of technical modifications to their systems – such technical modifications may be different for different countries around the world, which is a concern for SMPs who offer their services globally, as it creates technical complexity within networks.
- Concern over possible exposure of SMPs to legal liability.
- Necessity of coordination with FCC and/or FEMA, which in turn may be perceived as a step towards further regulatory activity.
- Some forms of activities by SMPs through the delivery of emergency alerts over social media may be deemed intrusive by their users.

SMPs can help with social media alerting in a variety of possible ways, including but not limited to the following:

- Providing mechanism(s) for authenticating the alert message to the citizen (e.g., using special symbols).
- Using their global view of message flows to detect messages containing inaccurate information and/or malicious information.
- Managing opt-in/opt-out lists.
- Automatically making a social media user a subscriber to all alerting accounts covering their geographic area (similar to but not the same as cooperation model).
- Assisting in geo-targeting, with the possibility of forcing the alert onto all users within an affected area.

- Prioritizing internal processing of traffic related to social media alerting – with emergency alerts time is of the essence, so the faster the emergency alerts are delivered the better.

6.4.1 Social Media Apps

In many if not all cases, direct intervention by the SMP can be substituted by an app on the *alerting account*. Examples include an app that monitors the feed from an Alert Aggregator and an app that manages opt-in/opt-out lists.

6.4.2 Large number of Alert Originators

There are thousands of authority personnel in the United States (federal, state, local, and tribal) who legitimately qualify as Alert Originators. The large number of potential Alert Originators in the U.S. poses at least two challenges to an SMP that wants to intervene in the delivery of emergency alerts over social media:

- Challenge 1: The SMP potentially would need to coordinate with thousands of emergency managers.

- Challenge 2: The SMP potentially would need to deal with multiple data formats for communications with different Alert Originators.

Both challenges would be greatly mitigated (and arguably eliminated), if SMPs only needed to interface with one AA using a single well-defined data format. The AA would absorb the burden of forging business relationships as well as identity verification, authentication, and authorization of AOs. By communicating with an AA, the SMP need only speak the data format "language" of that AA – preferably that data format is CAP, which has become the de-facto standard for emergency alert messages.

6.4.3 Mitigation of Challenges Through Virtual Volunteer Programs

Establishment of virtual volunteer programs may assist with the handling of social media workload and "crowd sourcing" of information related to public alerting. Moreover, such programs can improve situational awareness, identify falsely reported hazards, identify areas where misinformation amongst the general public requires correction in future alert updates, and ultimately save lives. Due to the level of service provided, such programs may also increase trust and credibility by the public with the emergency management office and related community decision leaders.

The American Red Cross has a virtual volunteer program for social media as part of its Digital Operation Center. Also, NOAA has experience with volunteer reporting programs, such as through its National Weather Service Storm Spotter program, which uses conventional telephone and email technology for citizen reporting and validation of weather related hazards and warnings.

Governmental organizations and emergency managers could study the models of the American

Red Cross and NOAA in regard to training and certification of volunteers for virtual volunteer programs related to social media and emergency alerting.

7 Working Group 2 Recommendations

7.1 Common Alerting Protocol (CAP)

For a federal architecture to achieve interoperability and information sharing, it is necessary to have an autonomous system to ensure everyone "speaks the same language." CAP does this. Accordingly, WG2 recommends the following:

- The FCC should strive to protect CAP from fragmentation while allowing industry groups to create their own profiles, possibly by ensuring the CAP Prime is constantly and frequently updated to subsume any major emerging profiles.
- The FCC should continue to encourage the adoption of CAP data format for all alerting technologies while facilitating its continued evolution to accommodate emerging needs of various stakeholders in the field.
- The FCC should recommend that the CAP protocol in the future be extensible to support specifications of new attributes/elements of various data types by the user community.
- The FCC should recommend that the CAP protocol in the future be able to communicate "soft error" messages to indicate non-adherence to specific profiles despite adherence to CAP.
- The FCC should continue to work with FEMA to encourage all State, Local, Tribal and Territorial governments to pressure vendors to use CAP. Consideration should be made for restricting federal funds for alerting technologies contingent on CAP compliance.
- Additional recommendations for best practices for implementing CAP-based alerts for consumer electronics devices may be found in CEA-CEB25, *Best Practices for Implementing Common Alerting Protocol (CAP) based Alerts for Consumer Electronics Devices*.

7.2 Alerting Architecture

Assuming concurrence with the concept that a federated architecture plays an important role in the introduction and widespread deployment of new alert dissemination technologies, the FCC should work with Congress and/or FEMA to seek the allocation of federal funding to implement and sustain emergency alerting federated architecture for the US public. One example would be to fund the IPAWS-OPEN aggregator.

7.3 Alert Origination, Aggregation and Dissemination

WG2 recommends the following:

1. A great deal of confusion exists about the allowable powers of AOs. When origination is limited to governmental agencies, control and training can be standardized. As the group of AOs grows and extends past the bounds of emergency managers and NOAA, some type of monitoring and authorizing of AOs will be necessary. Therefore, the FCC should work with FEMA to develop a hierarchical process whereby each "parent" node can empower "children" nodes and whereby the "parent" nodes are restricted to controlling

or influencing only the area for which they are responsible.

2. The FCC should encourage ADs and AAs to implement the NIST recommended practice of conducting CAP specification compliance and CAP profile conformance assessment on any new equipment.

3. The FCC should discuss with ADs the conditions under which it would be acceptable for ADs to "trim" alerts of high bandwidth consuming multimedia content for the sake of keeping the AD network/infrastructure operational.

4. The FCC should study in more detail the use of single versus multiple alert aggregation systems (refer to section 5.2.3 for details).

7.4 Device Manufacturers

WG2 recommends the following:

1. The FCC should encourage vendors of Alert Origination systems to leverage decision support and artificial intelligence technologies to populate automatically certain fields on the CAP message on behalf of the AO. This process would include the integration of hazard predictors for natural and man-made incidents. An example would be the full incorporation of downwind hazard prediction models to generate alert polygons and originate alert messages. This should also include the generation of multimedia alerts (e.g., if no audio file is explicitly included, then it generates one using text-to-speech technology).

2. The FCC should encourage the use of open-source software components to facilitate the implementation of alerting, including Mobile EAS alerts, for broadband devices. The FCC should also consider offering incentives for device manufactures to implement the alerting voluntarily.

3. Reinforcing the current vision of FEMA IPAWS, the FCC should encourage industry in general and device manufacturers in particular to integrate multiple alert technologies on devices to improve the reliability and opportunity to receive the alert message.

4. Recognizing that some entrepreneurially-driven next-generation alert dissemination technologies will not be commercially viable without funding for R&D and/or financial subsidies for deployment, the FCC should encourage Congress to provide funding to support new alert dissemination technologies through FEMA grants.

5. The FCC should encourage the establishment of a program and accompanying logo which certifies a public alerting application as providing alert information from official trusted sources, such as FEMA IPAWS or NOAA feeds. The program could be established by government, industry, or through a government-industry partnership.

6. The FCC should establish a consumer friendly rating (or levels), certification, and accompanying logo which identify the specificity of geo-targeting provided by an alert

application- particularly mobile devices. For example, the rating system could have 3 levels.

- Level 1 - The application alerts the user when the user is in the threat area. This means the user can be alerted when the user's point location or user configurable point location is within the alert polygon or circle when a polygon or circle is defined in the CAP message.

- Level 2 - The application alerts the user when the user is approximately in the threat area. This means the user can be alerted when the user's location is specified at the sub-county level (e.g., zip code, city, etc.) and overlaps the alert polygon or circle when a polygon or circle is defined in the CAP message.

- Level 3 - The application alerts the user when user may be in the threat area. This means the user can be alerted when the user's location is specified at the county level or better and overlaps the alert geo-code (i.e., county) defined in the CAP message.

7.5 Technology

WG2 recommends the following:

1. The FCC should recognize that market forces alone may not bring about new alert dissemination technologies that benefit the nation. One prior example of this is CMAS; another is the prospect of broadband alerts, which is mentioned in FCC's Broadband Plan as a desired alert dissemination method in the future.

   The FCC should take an active role in developing a strategic plan for identifying and deploying such technologies. This could include:

   - Creating consortiums or standards bodies to enable key stakeholders to work together for the purposes of helping to formulate and ultimately to implement the strategic plan.

   - Putting reasonable policies in place, aimed at removing regulator/legal barriers to the deployment of such technologies.

2. The FCC should encourage developers of alert origination systems to focus on how to better carry metadata such as targeted geographic area and authoritative URL for a landing webpage as it traverses the alert activity chain.

7.6 Access and Functional Needs

WG2 recommends the following:

1. As the FCC continues to evaluate the benefit of an action aimed at enhancing the efficacy of social media alerting for persons with disabilities, the FCC should perform the evaluation separately for each group and subgroup within the overall access and

functional needs community.

2. The FCC should conduct surveys of existing CSA technologies to identify those best suited for social media consumption and continue to promote research and development for technologies for automatically converting text emergency alert messages into multimedia messages, including sign language translation. Research should also be conducted to develop technologies for reformatting complex emergency alert messages into simple text.

3. The FCC and FEMA should offer grants to alerting system developers who will render CAP content in new ways that increase accessibility for people with disabilities.

7.7 Social Media

WG2 recommends the following:

1. The FCC should encourage the development of standardized training programs for emergency managers on Social Media Alerting. This program should be current, comprehensive, relevant, and reflect best practices for different types of communities and jurisdictions.

2. The FCC should produce a strategic vision for IT/Internet tools that support SM alerting and make it available to the public through an authoritative source. The vision should be communicated to AOs and be part of the Social Media alerting training program.

3. The FCC should discuss the feasibility, practicality and policy related challenges related to ISP assisted Geo-targeting of Social Media alerts with ISPs and SMPs. They should engage SMPs regarding enhancing their mobile apps to geo-target emergency alerts transmitted over social media. They should also open discussions on the possibility, challenges, and costs of opting in all users to federal *alerting account.*

4. The FCC should encourage the development of and help acquire government funding for developing innovative technologies for handling crowd-sourced inaccurate information.

5. The FCC should encourage government and emergency management organizations to consider adoption of virtual volunteer programs to ensure the operability, reliability, and resilience of social media for public alerting.

7.8 Future Alert Dissemination Technologies

WG2 recommends the following:

1. The FCC should coordinate with the industry to provide recommendations for the next version of CMAS, taking into consideration the recent advances in mobile devices (i.e., the advent of smartphones), as well as cellular networks (i.e., the ongoing migration to 4G networks) and Mobile EAS (CAP alerts delivered to mobile devices over Mobile DTV broadcasting).

2. The FCC should clearly define the goals, objectives, and targets for Broadband Alerting technology and erect a voluntary consortium body, similar to the CMAS body that consists of ISPs, with the understanding that ISPs play a similar role to TV and Radio stations. This consortium body would be charged to develop a unified plan and set of standards and practices for deploying Broadband Alerting to ensure that citizens across the U.S. are capable of receiving Broadband Alerts at the same service level. The FCC also should work to develop rules and regulations that address ISP concerns about legal liabilities and public perception related to delivering Broadband Alerts.

3. The FCC should continue to encourage the development of new technologies for alerting, while stressing the importance of sustaining existing alert and warning platforms as well. Our population continues to rely on a wide variety of technologies to communicate, and most people seem wed to one system or another. Eliminating one platform for another risks losing contact with a portion of our citizens. The best way to mitigate this is to preserve current technologies while developing new platforms for the future.

4. The FCC should also study and report on lessons learned from recent disasters, including the 2011 Great Earthquake and Tsunamis in Japan, severe tornados and wildfires in the U.S., as well as Superstorm Sandy.

5. The FCC should prioritize communication and coordination with other government agencies which are examining similar issues and holding workshops and seminars and/or issuing reports regarding developments in alerting theory, protocols, and technology, including without limitation the Department of Homeland Security Science and Technology Directorate, the National Academy of Sciences, and the Congressional Research Service.

Appendix A – Acronyms

This appendix defines the acronyms used within this report.

Acronym	***Definition***
3GPP	3rd Generation Partnership Project
AA	Alert Aggregator
AD	Alert Disseminator
ANSI	American National Standards Institute
AO	Alert Originator
ATIS	Alliance for Telecommunications Industry Solutions
ATOCA	Authority to the Citizen Alert
ATSC	Advanced Television Systems Committee
AWARE	Alerts, Warnings & Response to Emergencies
AWSM	Alerts and Warning Using Social Media
CAP	Common Alerting Protocol
CMAS	Commercial Mobile Alert System
CMSAAC	Commercial Mobile Service Alert Advisory Committee
CMSP	Commercial Mobile Service Provider
CSA	Computer/Smartphone Accessibility
CSRIC	Communications Security, Reliability and Interoperability Council
DHH	Deaf and Hard of Hearing
DHS	Department of Homeland Security
DHS S&T	Department of Homeland Security Science and Technology Directorate
DigiDOC	Digital Operations center
DOC	Disaster Operations Center
DOCSIS	Data Over Cable Service Interface Specification
DSL	Digital Subscriber Line
DTV	Digital Television
EAN	Emergency Action Notification
EAS	Emergency Alert System
EDXL	Emergency Data eXchange Language
ETN	Emergency Telephone Notification
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
GPS	Global Positioning System
IETF	Internet Engineering Task Force
IP	Internet Protocol

Acronym	***Definition***
IPAWS	Integrated Public Alert and Warning System
IPAWS-OPEN	Integrated Public Alert and Warning System Open Platform for Emergency Networks
ISP	Internet Service Provider
ITU	International Telecommunications Union
LP1	Local Primary One
LP2	Local Primary Two
M-EAS	Mobile Emergency Alert System
MDTV	Mobile Digital Television
MVPD	Multichannel Video Programming Distributor
NOAA	National Oceanic and Atmospheric Administration
NWS	National Weather Service
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Open Geospatial Consortium
PD	People with Disabilities
PEP	Primary Entry Point
PN	Participating National
POTS	Plain Old Telephone Service
R&D	Research and Development
RF	Radio Frequency
SMAC	Social Media Alerting Committee
SME	Subject Matter Expert
SMP	Social Media Provider
SMS	Short Message Service
TCP/IP	Transmission Control Protocol/Internet Protocol
TIA	Telecommunications Industry Association
URL	Uniform Resource Locator
VoIP	Voice Over Internet Protocol
WEA	Wireless Emergency Alerts
WG	Working Group
XML	Extensible Markup Language

Appendix B - Glossary

This appendix contains the glossary associated with this report.

Term	Definition
3GPP	The 3rd Generation Partnership Project (3GPP) is a collaboration agreement that was established in December 1998. The collaboration agreement brings together a number of telecommunications standards bodies which are known as "Organizational Partners".
Alliance for Telecommunications Industry Solutions (ATIS)	A U.S.-based organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. http://www.atis.org/
American National Standards Institute (ANSI)	Entity that coordinates the development and use of voluntary consensus standards in the United States and represents the needs and views of U.S. stakeholders in standardization forums around the globe. http://www.ansi.org/
American Standard Code for Information Interchange (ASCII)	A standard for defining codes for information exchange between equipment produced by different manufacturers. A code that follows the American Standard Code for Information Interchange.
Call	A session established by signaling with two way real-time media and involves a human making a request for help. We sometimes use "voice call", "video call" or "text call" when specific media is of primary importance. The term "non-human-initiated call" refers to a one-time notification or series of data exchanges established by signaling with at most one way media, and typically does not involve a human at the "calling" end. The term "call" can also be used to refer to either a "Voice Call", "Video Call", "Text Call" or "Data–only call", since they are handled the same way through most of NG9-1-1.
Carrier	A function provided by a business entity to a customer base, typically for a fee. Examples of carriers and associated services are; PSTN service by a Local Exchange Carrier, VoIP service by a VoIP Service Provider, email service provided by an Internet Service Provider.
Enhanced 9-1-1 (E9-1-1)	A telephone system which includes network switching, data base and Public Safety Answering Point premise elements capable of providing automatic location identification data, selective routing, selective transfer, fixed transfer, and a call back number. The term also includes any enhanced 9-1-1 service so designated by the Federal Communications Commission in its Report and Order in WC Docket Nos. 04-36 and 05-196, or any successor proceeding.
Gateway	The Point at which a circuit-switched call is encoded and repackaged into IP packets – Equipment that provides interconnection between two networks with different communications protocols.
Geo-coding	Translation of one form of location into another, typically a civic address into an x,y coordinate.
Geo Location	Latitude, longitude, elevation, and the datum which identifies the coordinate system used.
Geospatial	Data accurately referenced to a precise location on the earth's surface.
Global Positioning System (GPS)	A satellite based Location Determination Technology (LDT).

Term	Definition
Instant Messaging (IM)	A method of communication generally using text where more than a character at a time is sent between parties nearly instantaneously
Internet Engineering Task Force (IETF)	Lead standard setting authority for internet protocols.
Internet Protocol (IP)	The method by which data is sent from one computer to another on the Internet or other networks.
Internet Service Provider (ISP)	Company that provides Internet access to other companies and individuals
Jurisdiction	A government agency that has contracted for Enhanced 9-1-1 service. This may be a county, a city, a COG, or a 9-1-1 Area.
Location	In the context of location information to support IP based emergency services: The physical position of VoIP end-point expressed in either civic or geodetic form. A spot on the planet where something is; a particular place or position. Oxford Dictionary, Oxford University Press, 2009.
Telecommunications Device for the Deaf (TDD)	Also known as TTY. (see Teletypewriter (TTY))
Telecommunications Industry Association (TIA)	A lobbying and trade association, the result of the merger of the USTA (United States Telephone Association) and the EIA (Electronic Industries Association).
Telecommunications Relay Service (TRS)	A federally mandated service provided by states that provides communication relay between TTY users and voice telephone users, via a third party, for communications assistance.
Teletypewriter (TTY)	Also known as TDD. A device capable of information interchange between compatible units using a dial up or private-line telephone network connections as the transmission medium. ASCII or Baudot codes are used by these units. (per EIA PN-1663)
Text Telephone	Another term for TDD/TTY
Third Generation Partnership Project 2 (3GPP2)	A collaborative third generation (3G) telecommunications specifications-setting project comprised of interests from the Americas and Asia developing global specifications for Mobile Application Protocol (MAP) "Wireless Radio-telecommunication Intersystem Operations" network evolution to 3G. The project is focused on global specifications for the radio transmission technologies supported by MAP and the wireless IP core networks, together known as the cdma2000® family of standards.
Working Group (WG)	A group of people formed to discuss and develop a response to a particular issue. The response may result in a Standard, an Information Document, Technical Requirements Document or Liaison.
x, y	Shorthand expression for coordinates that identify a specific location in two dimensions representing latitude and longitude.

Appendix C - Different Options for Alert Aggregation

Figure 11 shows a generic federated architecture, while purposefully emphasizing the fact that there are different options for the alert aggregation box. It is also important to note that the architecture does not preclude direct connectivity between AOs and ADs.

For example, as depicted in Figure 12, alert aggregation can be performed by a single AA, which in the future may or may not be IPAWS-OPEN.

Figure 13 shows a possible architecture with multiple AA's. In this scenario, private sector AA's would be competing for the business of AOs and ADs.

Figure 14 shows that in the case of multiple aggregators they may be organized hierarchically. This for example may be a natural way of organization that mirrors the hierarchy of *local-state-federal jurisdictional* hierarchy. It may be also be possible to have aggregators dedicated to certain types of Alert Originators or certain types of locales (e.g., college campuses). If multiple AAs are indeed available to AOs and ADs, then having a definitive and comprehensive directory for the AAs would be helpful.

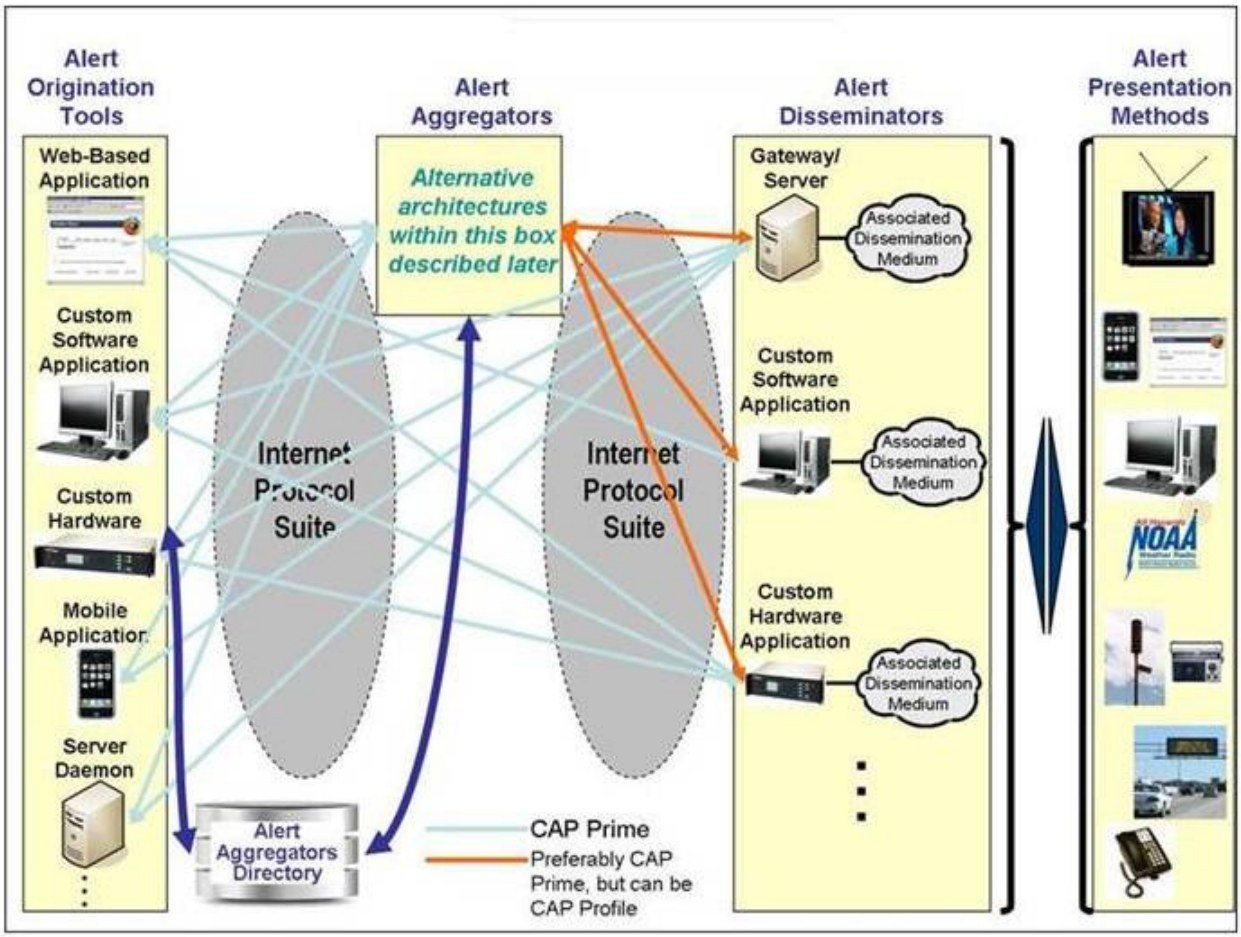

Figure 11 – Generic Federated Architecture for Emergency Alerting

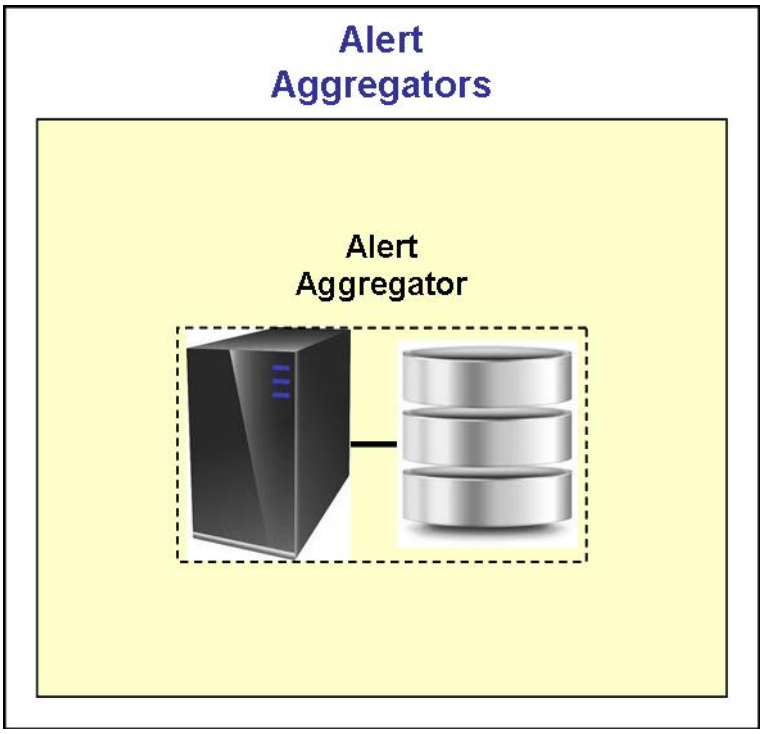

Figure 12 – Alert Aggregation Performed by a Single AA

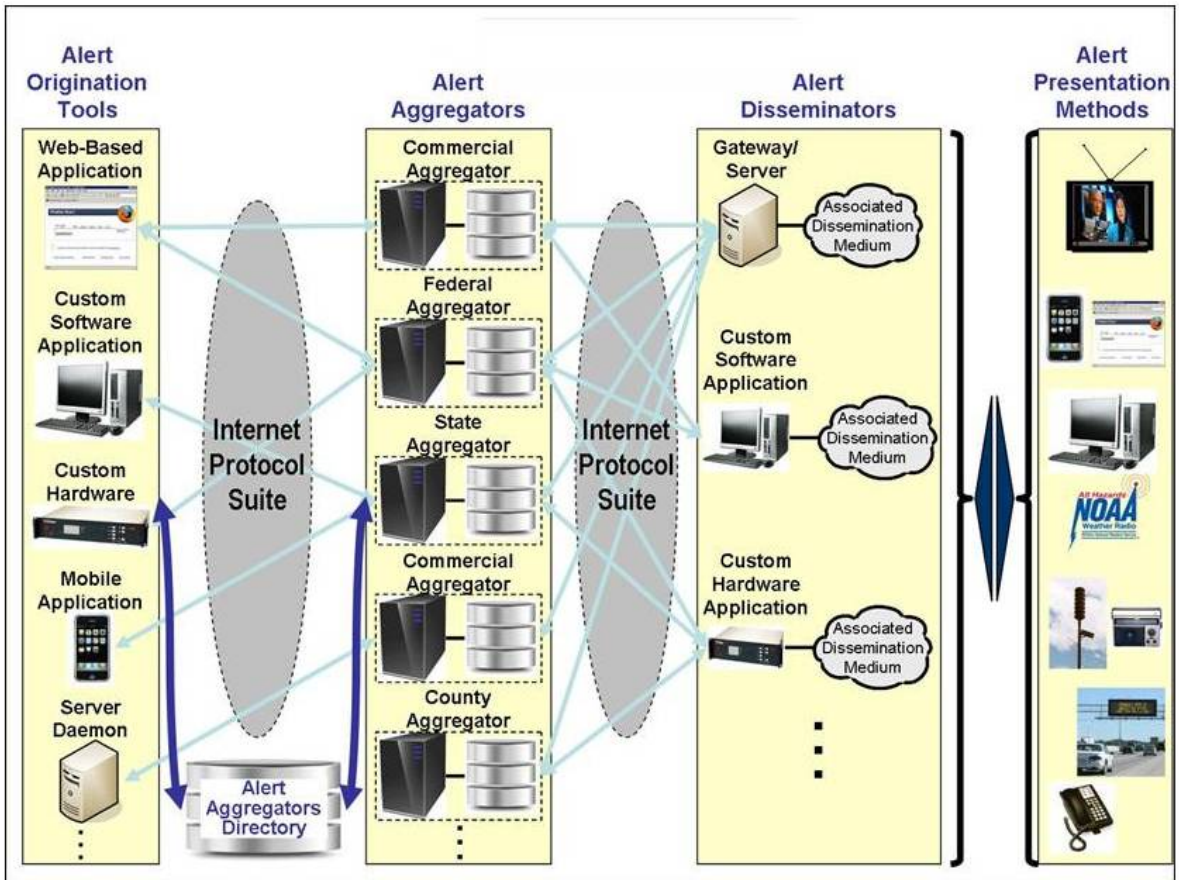

Figure 13 - Alert Aggregation Performed by Multiple Aggregators in Parallel

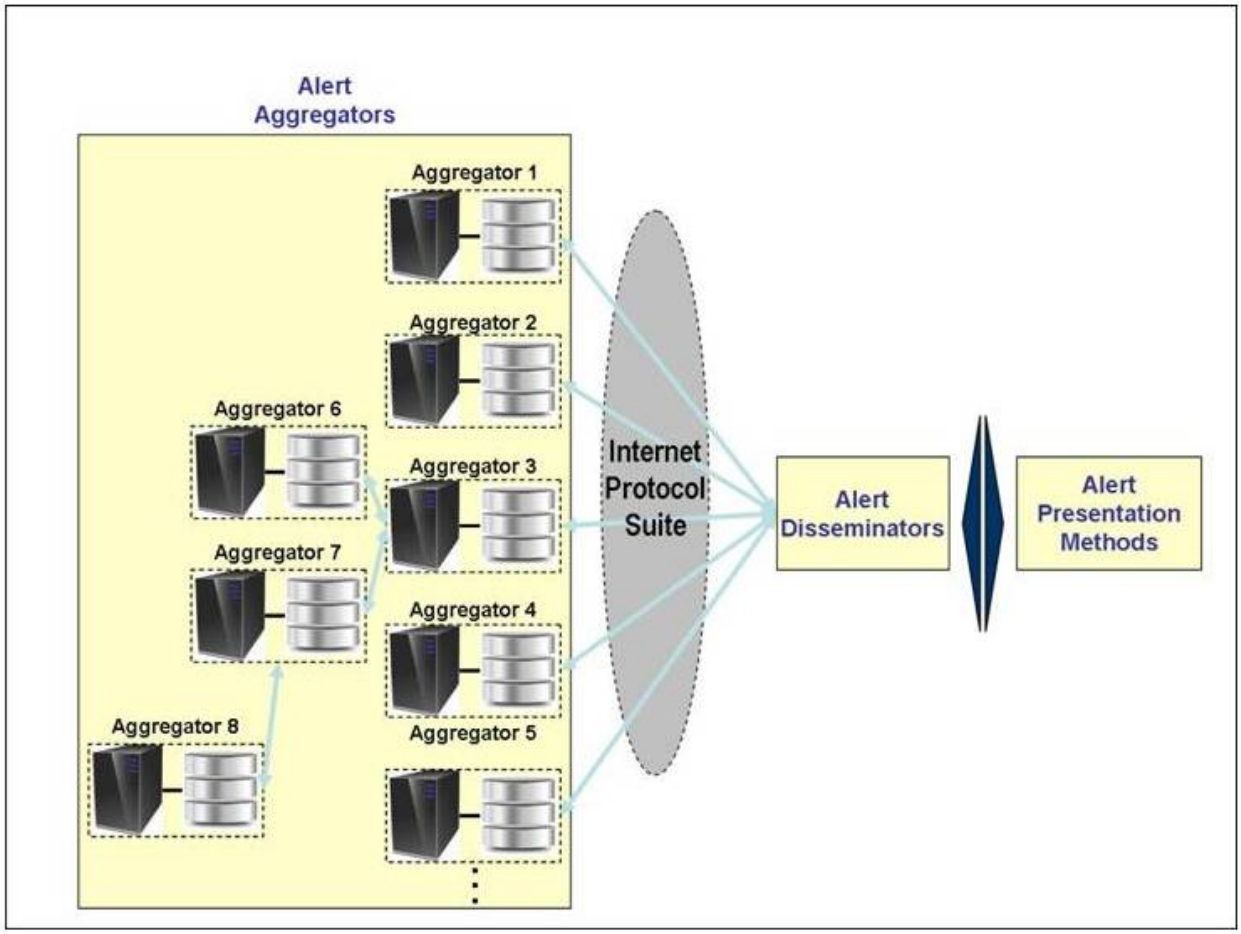

Figure 14 – Alert Aggregation Performed by Multiple Aggregators, Some in Parallel and Some Organized Hierarchically

The Value of Alert Aggregation

In theory, the Alert Aggregator is not necessary in the federated architecture. Given the ubiquitous presence of the Internet, AOs and ADs can communicate directly over the Internet or satellite. In addition to the Alert Aggregators not being operationally necessary, there are at least four arguments against having Alert Aggregators.

First, since one the primary metrics of public alerts is the length of time it takes for the public to receive the alert, one argument against alert aggregation is that it introduces time delay. However, this counter argument may be more perceived than actual. No one is claiming that either EAS or CMAS (which today go through the IPAWS-OPEN aggregator) is failing on that point. Furthermore, the speed of digital communication is constantly improving, so even if delay issues did exist, they will disappear in the future. Finally, the time scale of any delay (even if current time delays persist) is minuscule (at most a few seconds), that it is highly unlikely to make a life-and-death difference (will sending an alert directly to Facebook save a few seconds, and if so will it make a life and death difference?)

Second, for some simple AD channels going through an AA can appear to be a roundabout way of transmitting an alert. For example, it can be argued that the ETN dissemination channel is not designed to deliver media-rich versions of the alert (e.g., video-based alerts) that would benefit

from the big TCP/IP data pipes and the CAP-format alert messaged likely to be associated with the AA. So ETN really does not need to go through an AA.

Third, the federal government cannot realistically mandate and enforce that all public alerts go through (an) Alert Aggregator(s). For example, there is nothing to stop schools or universities from using a third-party stovepipe alerting system.

Regarding the second and third arguments above, it is not expected that the AA-based federated architecture will be the only architecture for emergency alerting. It is possible for it to exist alongside several stovepipe architectures and possibly non AA-based federated architectures.

Fourth, if Alert Aggregators are standards-based, whereby standards may be influenced by the constraints of large infrastructures such as Cable, Radio, and Telecom, then changes to such standards would not be swiftly concocted or executed.

That said however, the AA component in the federated offers several practical advantages – so much so that ironically the alert aggregator in the federated architecture (for emergency alerts) is possibly the most critical component of the architecture. The AA performs several functions:

1. **Shared facility for a priori identity verification and authorization**: An alert message has such an impact on a community that it better have emanated from an emergency manager. The AA can perform a priori verification of the identity of the AO, and can verify that the AO is authorized to send out alerts (potentially with different authorization levels for different types of alert messages).
2. **Shared facility for authentication**: The AA can have in place mechanisms for verifying the authenticity of an alert message i.e., that it did indeed come from the AO that it claims it came from.
3. **Reduction of number of business relationships**: If AOs and ADs were to exchange messages directly in a point-to-point fashion; each AO-AD pair would have to forge a separate business relationship. Instead, the AOs can establish business relationships with the AA on one end, and the ADs can establish business relationships with AA on the other end. The total number of business relationships in this scenario would be significantly smaller in the latter scenario.
4. **Legal liability indemnification**: ADs may be wary of any legal liabilities connected with the dissemination of alerts to the public. The AA can indemnify ADs of such legal liabilities, as long as the ADs observe their agreements with the AA.
5. **Routing**: At a first glance, it may seem that the critical role that it plays is that of router – this would imply that the AO system would not know how to deliver the alert message to the AD, and therefore relies on the AA to route the alert message to the AD. However, this may be a misleading view. First, in the age of the Internet, it suffices for the AO to have the URL/IP address of the AD (or its gateway), and have the Internet perform the routing of the message to the AD. Knowledge of the AD's URL/IP address would certainly be the case, if the two entities have a business relationship. Nevertheless, it is conceivable that an AO would be interested in disseminating the alert message over TV airwaves for example, without knowing precisely which broadcast station(s) cover(s) their jurisdiction. In that case, the AA may play a routing role in the sense of resolving which broadcasting station(s) geographically correspond to the targeted alerting area.

By performing the functions above, the presence of the AA greatly reduces the barriers-to-entry for innovative value-adding AO systems and AD methods/technologies.

One key advantage of the federated architecture that would be enjoyed by emergency managers is the realistic possibility of having a single AO interface that activates all the AD systems simultaneously. This advantage is important in the immediate aftermath of an incident when every second counts. With stovepipe systems, the emergency managers lose time activating different systems from separate interfaces.

Conditions for a Successful Federated Architecture Centered on Alert Aggregation

For a federated architecture to indeed achieve interoperability and information sharing, it is would be greatly helpful if the autonomous systems within it "spoke the same language". In the case of emergency notification, speaking the same language requires:

1) Speaking the same networking language, and
2) Speaking the same language for the alert message

The path of least resistance for (1) is the Internet Protocol suite (e.g., TCP/IP). The path of least resistance for (2) is the CAP protocol.

The Internet Protocol suite is well-established with no danger of fragmentation.

The CAP protocol however does face the danger of fragmentation, as different industry groups may adapt it to their specific needs.

**Suggestions only, can be established by State EAS Plan*

Appendix D - EAS Illustrations – Differences between Classic Version and CAP/IPAWS

The illustrations below provide an overview of the classic EAS network and an introduction to the CAP/IPAWS network. In reviewing these drawings it can easily be seen that the CAP/IPAWS network complexity has increased, but will start allowing the capability to adapt the distribution and content of the alert communications because of geographic location, risks, or personal user preferences, as appropriate. This can be extended to those with disabilities and those without an understanding of the English language.

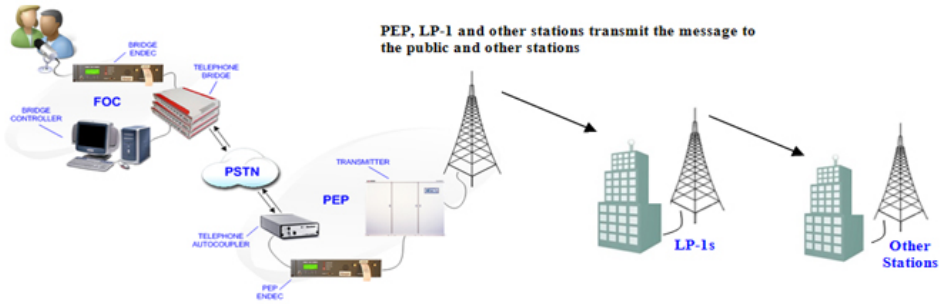

Figure 15 – Classic EAS Network

At present, the United States is divided into approximately 550 EAS local areas, each of which contains at least two Local Primary stations, designated “Local Primary One” (LP1), “Local Primary Two” (LP2), and so on. The LP stations must monitor at least two EAS sources for Presidential messages (including State Primary stations and in some cases a regional PEP station), and also can serve as the point of contact for state and local authorities and NWS to activate the EAS for localized events such as severe weather alerts. All other EAS Participants are designated Participating National (PN) stations and must monitor at least two EAS sources, including an LP1 and an LP2 station as specified in the state’s EAS plan.

Summary

The details, assumptions and conclusions presented in this paper are based on the current understanding of the deployed CAP/IPAWS system. As with any assumption, these are subject to change as the CAP/IPAWS system evolves.

This notwithstanding it has become apparent that the growth and evolution of the CAP/IPAWS system will be primarily controlled as the need arises. At this time the most effective way to control this type of expected changes is by establishing a Joint Users Taskforce that is charged with the management of the policy and procedure that surround the operation of the CAP/IPAWS system.

Through-out this document there have been recommendations made for hardware enhancements and the creation of supporting documents (best practices) establishing supporting policies. In the order of importance the documentation and polices are needed to support the currently deployed base of EAS alert providers. It is critical that the users of this network are trained and qualified to do so. It is also critical that the EAS and CMAS alert providers understand what their requirements are under the law, so that compliance is assured.

Appendix E - Relevant Example of SM in Emergency Management

In 2009, the American Red Cross commissioned a study which found that social media sites are the fourth most popular source to access emergency information. Social media are also commonly used by individuals and communities to warn others of unsafe areas or situations, inform friends and family that someone is safe, and raise funds for disaster relief.

Based in part on that study, the American Red Cross intensified is efforts in using social media in its emergency management-related operations. This section discusses the efforts the ARC with respect to using social media in emergency management.

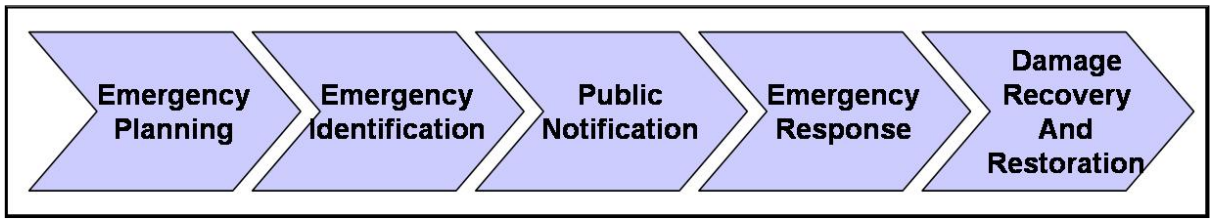

Figure 16 - High-level Activity Chain for Emergency Response, Planning and Management

Looking at Figure 16, although the ARC operates mostly in the "Damage Recovery and Restoration" phase, as opposed to the "Public Notification" phase, the use of social media has comparable facets with its use for alerts and warnings. Moreover, ARC seemingly has set the standard for the use of social media in emergency management, in terms leveraging advanced technologies as well as human volunteers; and also in terms of best practices for emergency-related human dialogue over social media. Indeed, the example of the ARC provides valuable lessons for the use of social media to deliver alerts and warnings.

Focusing on the advanced technology that ARC is currently using, the ARC has set up, within its headquarters' disaster operations center (DOC), a "Digital Operations Center" (DigiDOC).

DigiDOC is an area that is twenty feet long by eight feet wide, with three computers and six flat-panel displays on a wall, that provide visualization tools. DigiDOC It is staffed with three full-time employees, but leverages an army of off-premises volunteers. DigiDOC serves four purposes:

- It provides a single snapshot to DOC workers of what is happening on the social web during a given disaster using advanced visualization tools.
- The technology powering these visualizations gives us a bigger picture of situational awareness.
- It helps the ARC to begin anticipating the needs of an affected community, whether clients, donors, or others.
- It gives the ARC the ability to decentralize, whereby it allows the ARC to increase the number of people engaging citizens from the three full-time staff members to include subject matter experts (SMEs) in the DOC as well as digital volunteers, during high-demand periods. Both groups can be trained offline on how to engage the public. (The DOC SMEs can also help with building the digital volunteers base).

The figures below show the visualization tools which the ARC finds extremely valuable for its

social media operations.

Figure 17 shows the heat map, which shows volume of conversations about a given topic based on geography.

The Community screen in Figure 18 also shows tweets about a chosen topic profile – it helps one understand who is talking about a particular subject. The screen displays a random selection of tweets from the last 4 hours and displays them. The bigger the profile image on the screen, the more influence the person has. Influence is measured by the size of the person's following and also how often they have talked about this subject.

The Universe screen in Figure 19 displays several Topic Profiles in a sun-and-planet format. It shows results from the last 3 days. The "Sun" is the primary subject of each Topic Profile. The "Planets" are different groups of keywords within that broader subject that we've broken it down into. This visualization helps the ARC quickly see how many posts each subject group is pulling in and what the overall sentiment is.

The screen in Figure 20 displays a bigger picture dashboard where the ARC can see overall volumes of conversation over a number of days, our share of voice versus partners, and overall sentiment.

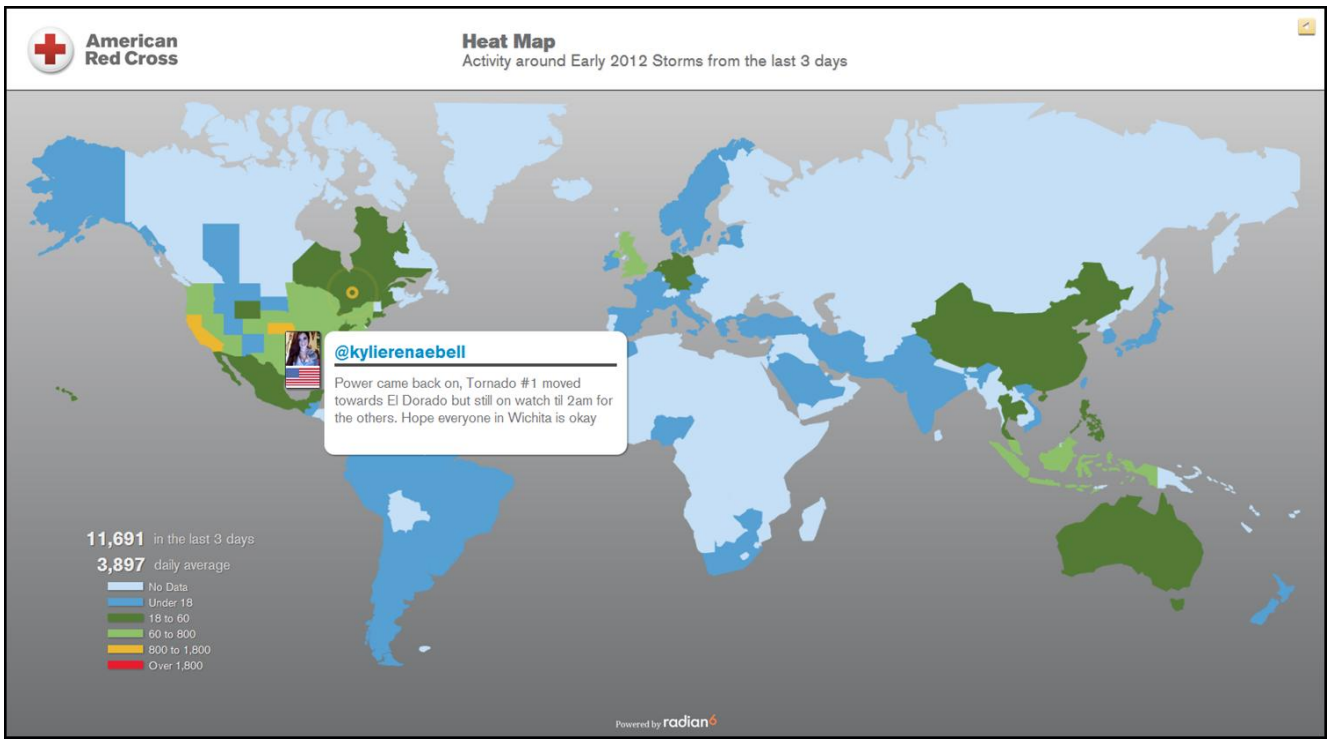

Figure 17 - Heat Map

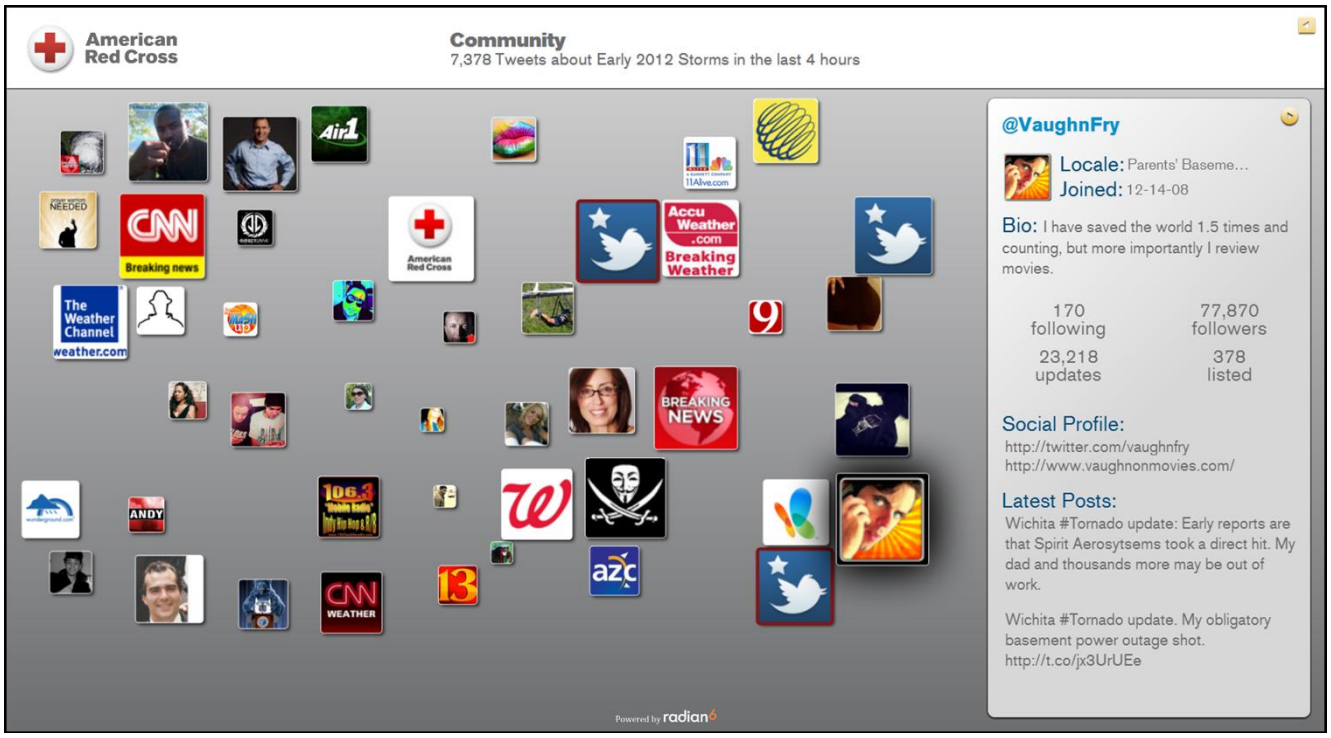

Figure 18 - Community Snapshot

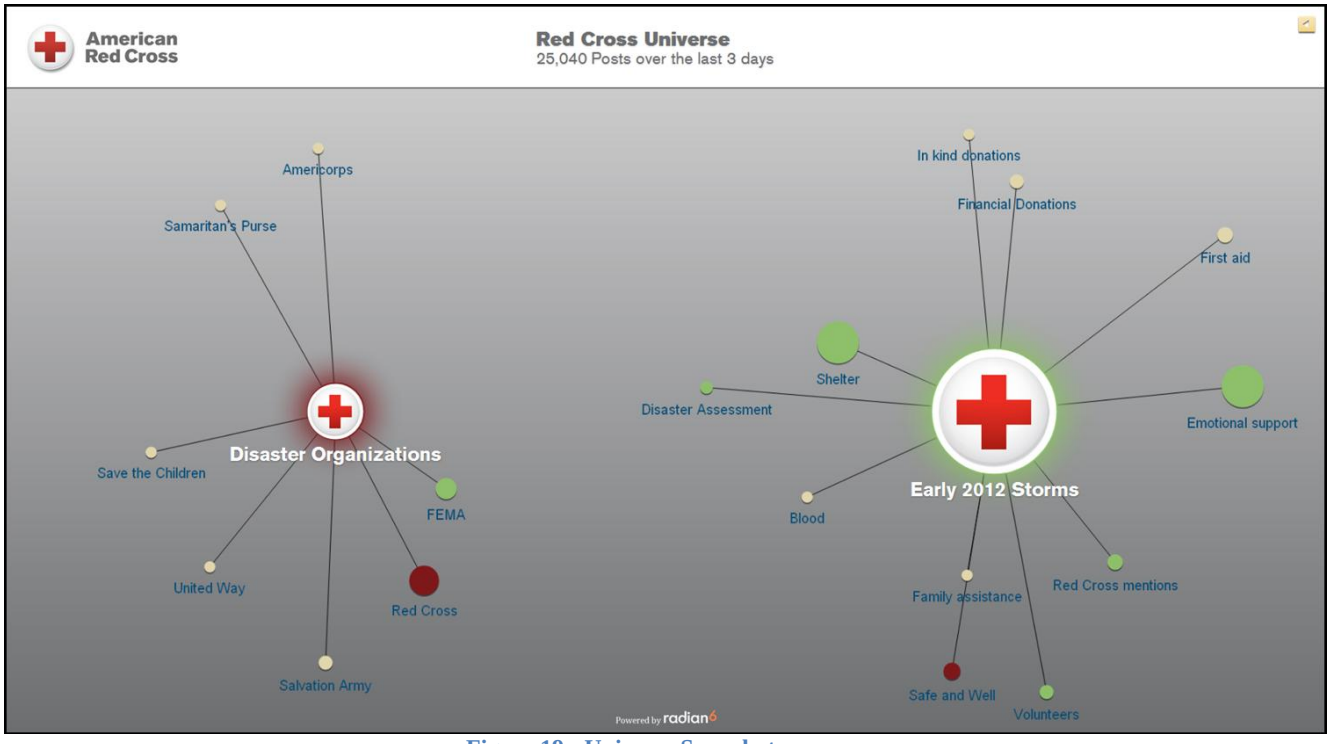

Figure 19 - Universe Snapshot

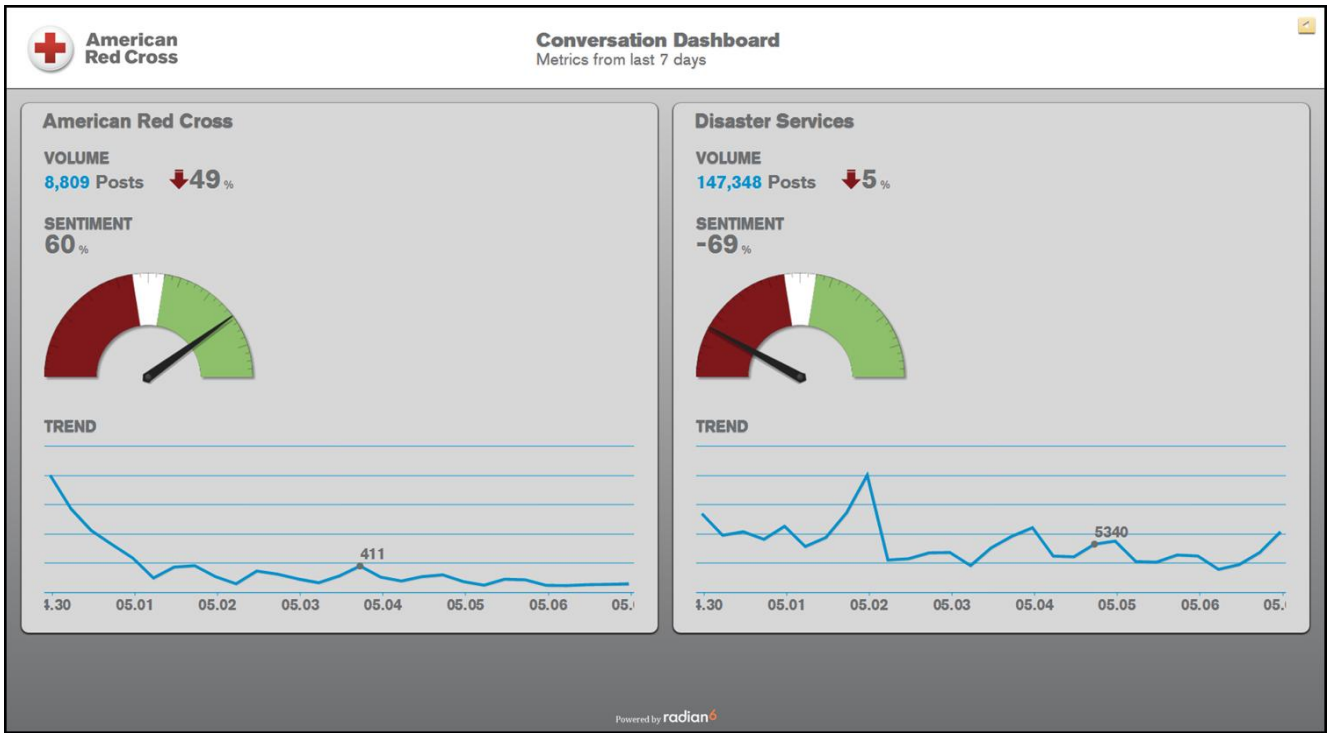

Figure 20 - Conversation Dashboard

It is important to note that the visualization tools are provided by a commercial provider, namely Radian6. The funding of DigiDOC, including the purchase of the Radian6 software, was provided by Dell. So as valuable as they are, the ARC would not have been able to afford the visualization tools by itself. In addition, the visualization tools required significant training (over a period of several months) for the staff using it. The ARC staff also invested significant amount of time providing feedback and working with to Radian6, for the latter to tweak it internal parameters of the visualization tools to reflect the priorities of the ARC.

Appendix F – About Broadband Alerting

Broadband Alerting warrants special attention because it was specifically mentioned in FCC's 2010 National Broadband Plan. The plan stated:

1- "*Broadband can also provide the public with new ways of calling for help and receiving emergency information*" and
2- "*A cutting-edge public safety communications system uses broadband technologies … to revolutionize the way Americans are notified about emergencies and disasters so they receive information vital to their safety.*"

In addition, the term Broadband Alerts is increasingly being thrown around in the emergency alerting community.

Definition of Broadband Alerts

One of the main challenges to understanding Broadband Alerting technologies is the **definition** of Broadband Alerts. The central question is:

If the alert is transported via Broadband, does that make it a Broadband Alert?

If the answer to that question is yes, then a whole class of technologies can be classified as Broadband Alerting technologies, making some technologies in use today classifiable as Broadband Alerts, which in turn arguably makes Broadband Alerting a reality today.

Comparison of Broadband Alerting Technologies

Table 7 below compares the different technologies that can possibly be classified as Broadband Alerting technologies under the most liberal definition. Before starting the comparison, the parameters of comparison are first established.

The comparison parameters are described in Table 6:

Parameter	Values	Explanation
Geo-targeting		No deliberate/explicit geo-targeting of alert
		Increasing degrees of precise definition of alert area and adherence to defined area when delivering alert
		
		
		Polygonal specification of alert area with 100% adherence in delivery
Subscription-Based	Yes	Citizen must subscribe to receive alerts
	No	Citizens receive alerts without having subscribed, unless explicitly opting out
Service/Device Customization	Yes	The service/device must be customized in a particular way to receive alerts e.g., software installation e.g., desktop alerts
	No	Out-of-the-box setup/configuration

		sufficient to receive the alert e.g., CMAS, EAS, Emergency Telephone Notification
Specific Service/Device Usage	Yes	The service/device must be used in a particular way to receive the alert e.g., a TV viewer must be tuned to a particular TV channel
	No	As long as the service/device is being used, the alert will be received

Table 6: Parameters for Comparing Arguable Broadband Alerting Technologies.

Table 7 provides a comparison of Broadband Alerting technologies.

Technology	Descriptive Figure	Argument	Geo-Targeting	Subscription-Based	Customization	Specific Usage
Broadband EAS	Figure 21 and Figure 22	o Delivered Broadband users on Desktops, laptops tablets as they use web-browsers and stream online multimedia o Intended to be delivered to end-users in a manner similar to traditional EAS – during normal consumption of service without subscription and without customization	●	No	No	No
Email	Figure 23	o Email received via the Internet o Internet access typically via Broadband	○	Yes	No	Yes
Social Media	Figure 24	o Social Media accessed via the Internet o Internet access typically via Broadband	○	Yes	No	No
Google Public Alerts	Figure 25	o Webpage requested and delivered via the Internet o Internet access typically via Broadband	○	No	No	Yes
Desktop/	Figure 26	o Installed	◑	No	Yes	No

Homescreen Alerts		application/app communicates with server via the Internet o Internet access typically via Broadband				
HTML5 Notification	Figure 27	o HTML5 notifications will be communicated via the Internet o Internet access typically via Broadband	○	?	Yes	Yes
Digital Cable Alerts	Figure 28	o Digital cable signal transmitted over a Broadband connect (coaxial cable, fiber, hybrid fiber coaxial)	●	No	No	No
Custom Mobile Apps	Figure 29	o Content data received over cellular data connection o 3G/4G cellular data connectivity considered by many to be Broadband speed	●[5]	No	Yes	Yes
Popular Websites	Figure 30	o Webpages requested and delivered via the Internet o Internet access typically via Broadband	○	No	Yes	Yes
Over-the-Top Streaming Media e.g., Hulu, ESPN3	Figure 31	o Streaming content delivered over the Internet o Internet access typically via Broadband	○	No	Yes	Yes
Popular web-content delivered via custom mobile apps	Figure 32	o Content data received over cellular data connection o 3G/4G cellular data connectivity considered by	●[6]	No	Yes	Yes

[5] Geo-targeting possible if location-based services not turned off. If they are, it is considered a form of opt-out.
[6] Geo-targeting possible if location-based services not turned off. If they are, it is considered a form of opt-out.

		many to be Broadband				

Table 7: Comparison of Arguable Broadband Alerting Technologies.

Broadband Alerting and Geo-targeting

Geo-targeting for Broadband alerts has turned out to be a different challenge for Wireless Broadband vs. Landline Broadband – not so much because of any inherent difference between the two technologies, but rather because wireless Broadband end-devices are increasingly GPS-capable which can be leveraged for geo-targeting (with certain limitations such as z-axis). In the case of landline Broadband, the ISP's intervention is necessary to deliver alerts in a geo-targeted fashion.

Descriptive Figures

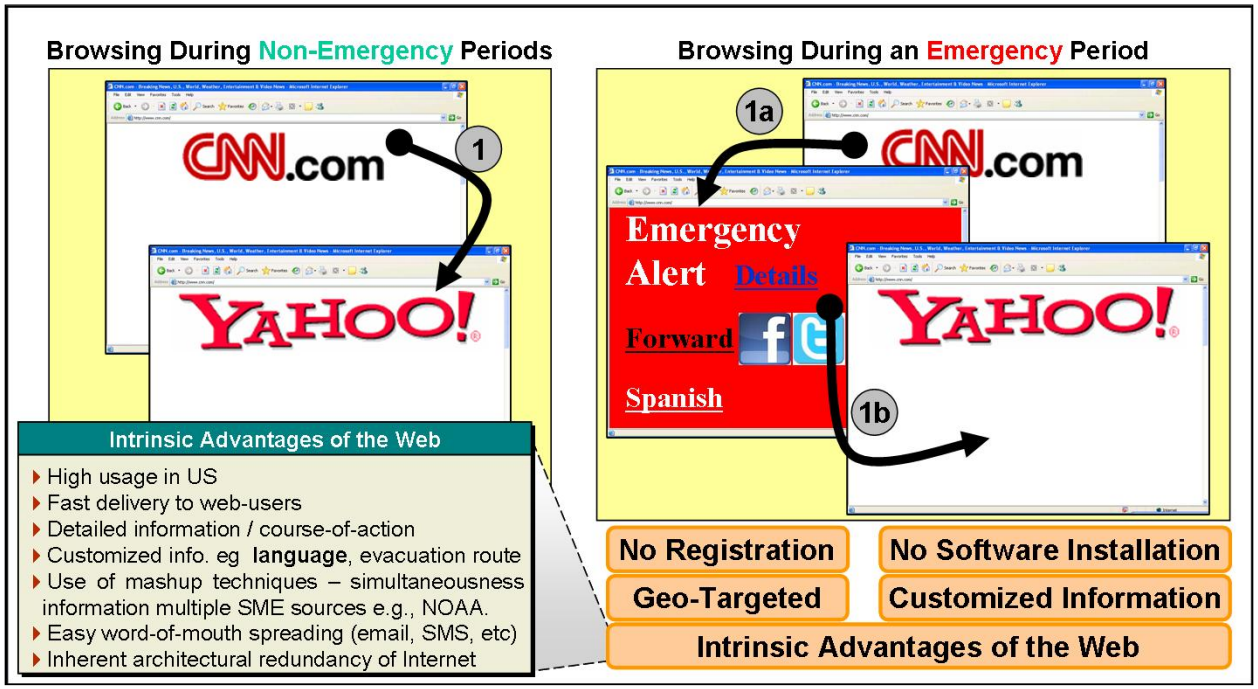

Figure 21: Broadband EAS for web-browsers.

Figure 22: Broadband EAS for streaming video.

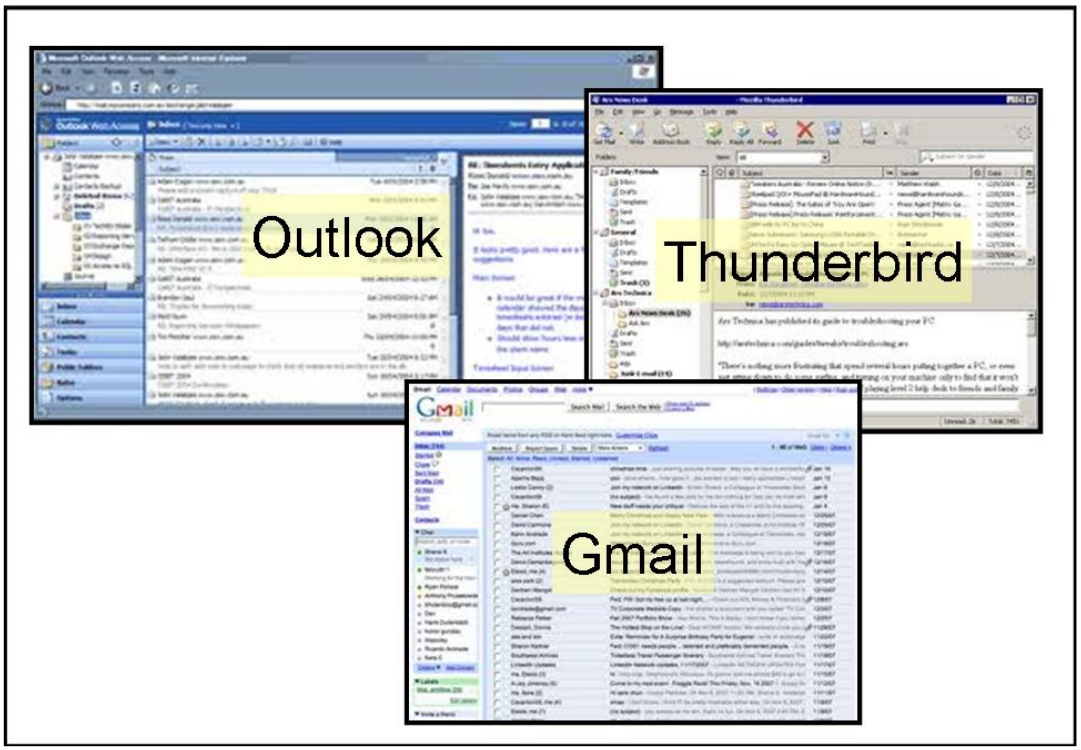

Figure 23: Email Broadband Alerts.

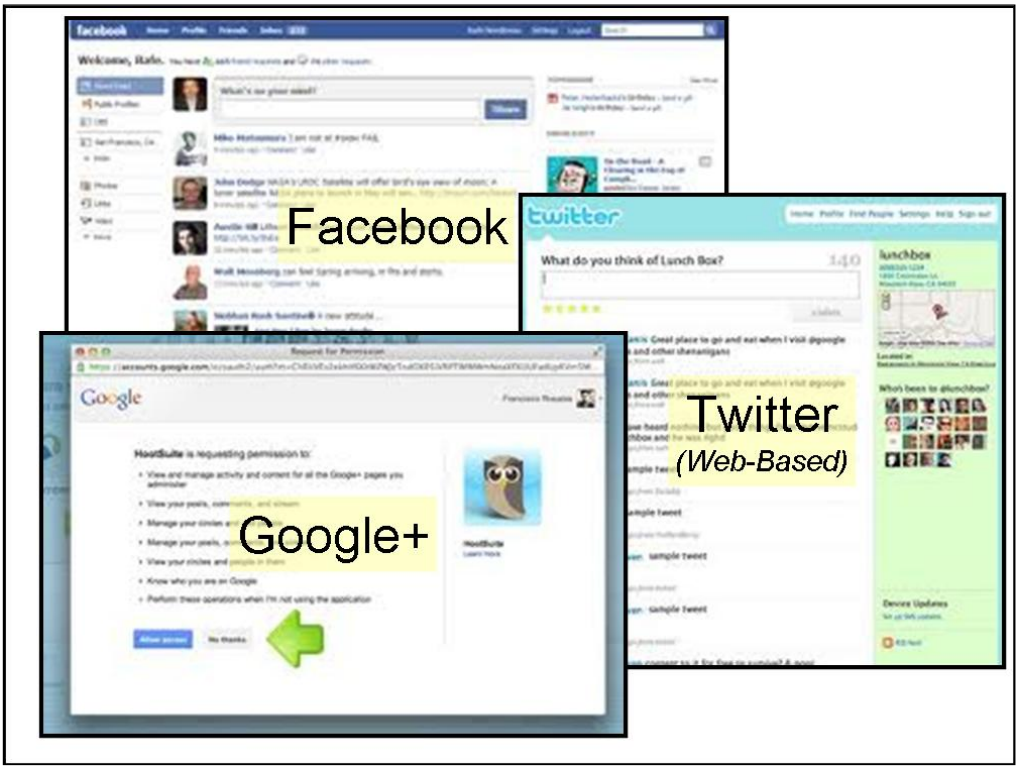

Figure 24: Broadband Alerting – Social Media Alerts.

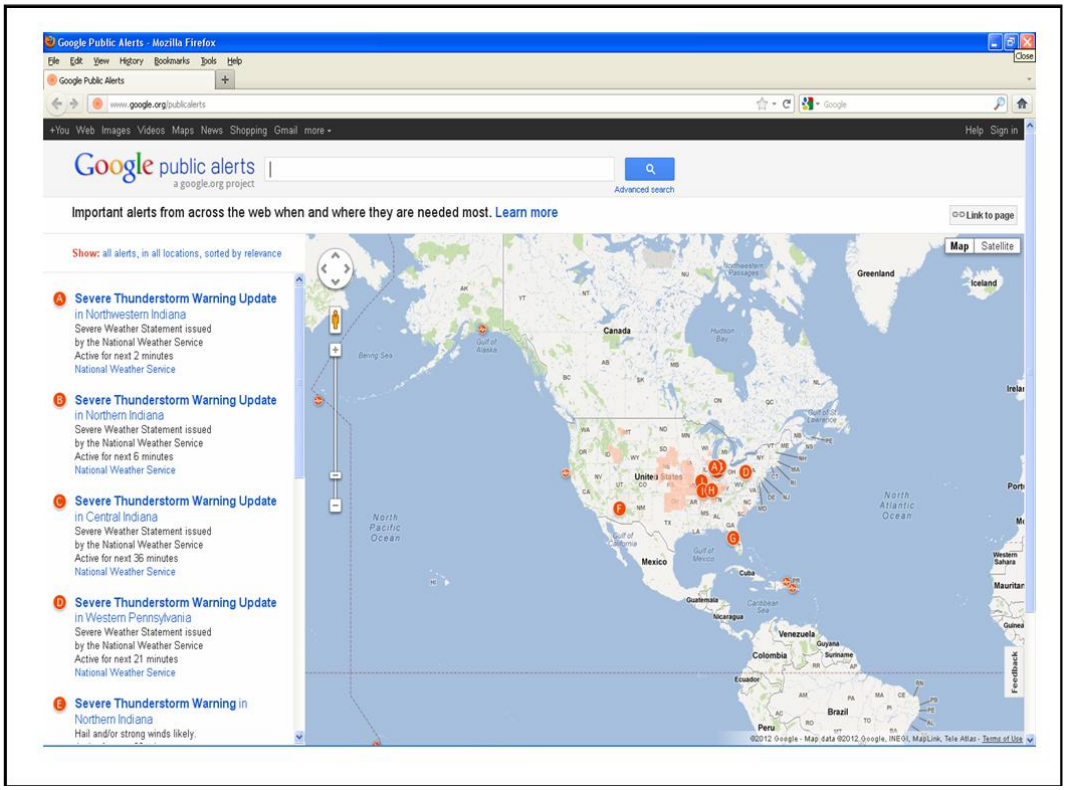

Figure 25: Broadband Alerting – Google Public Alerts.

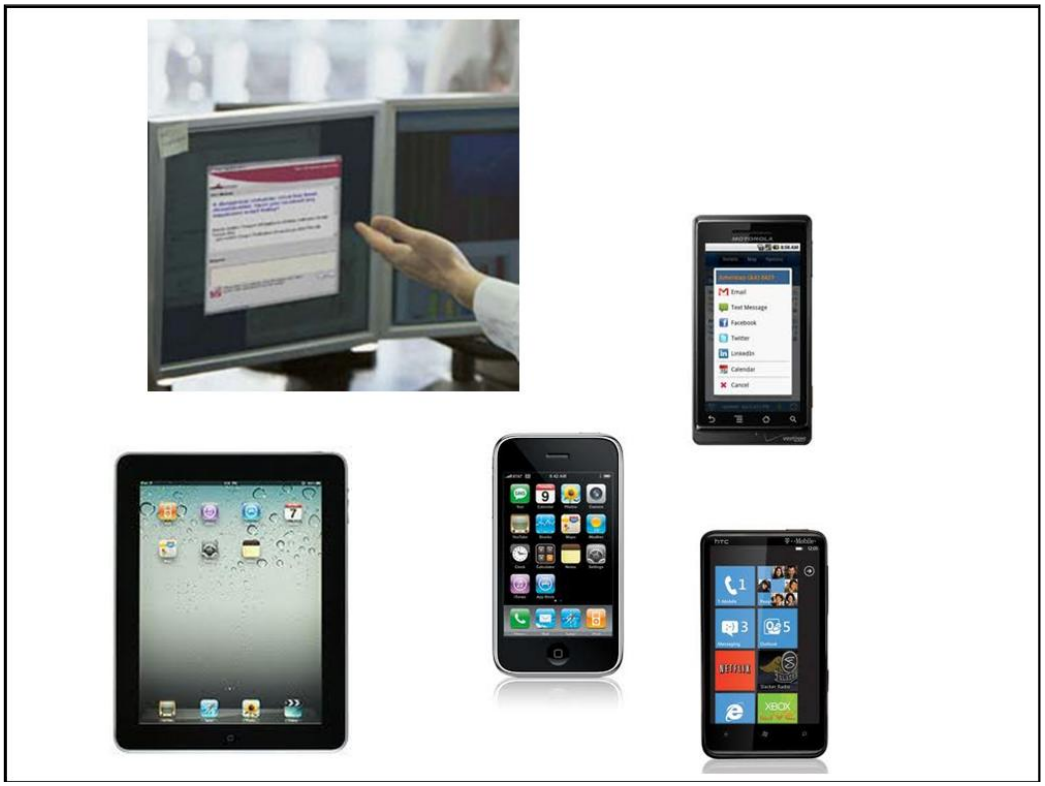

Figure 26: Broadband Alerting – Desktop/Homescreen Alerts.

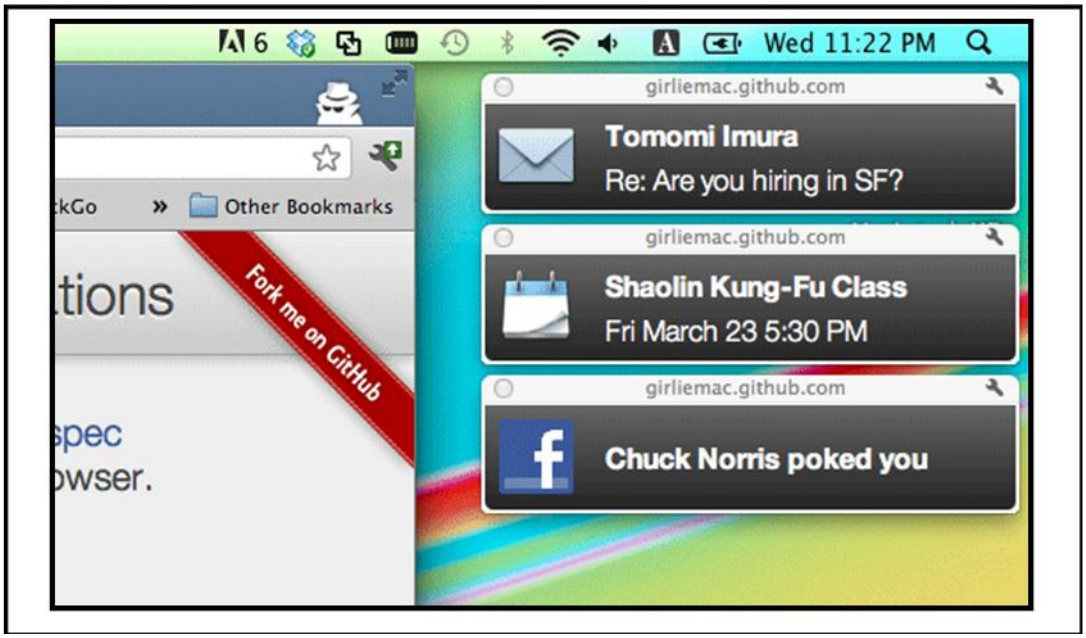

Figure 27: Broadband Alerting – Alerts via HTML5 Notification.

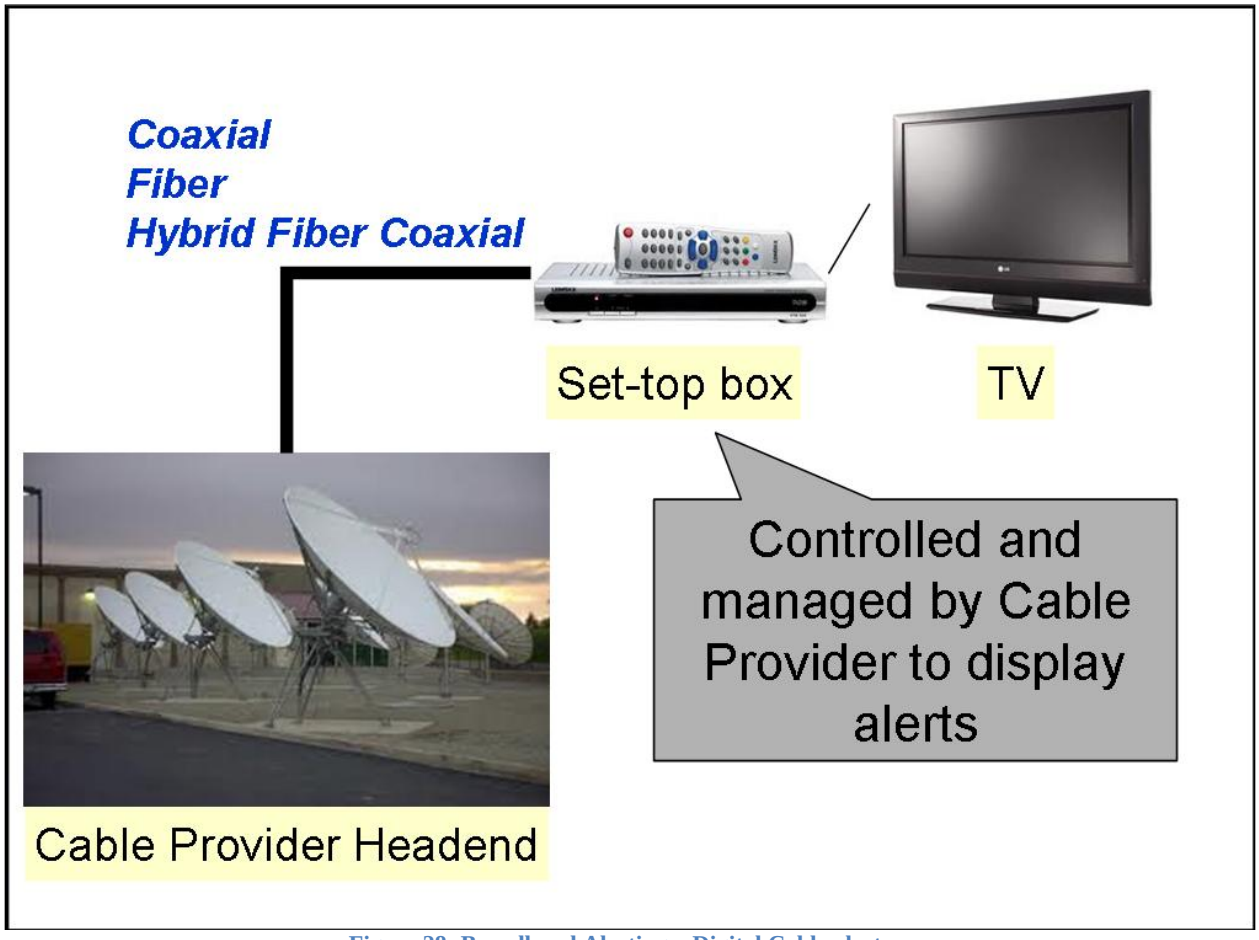

Figure 28: Broadband Alerting – Digital Cable alerts.

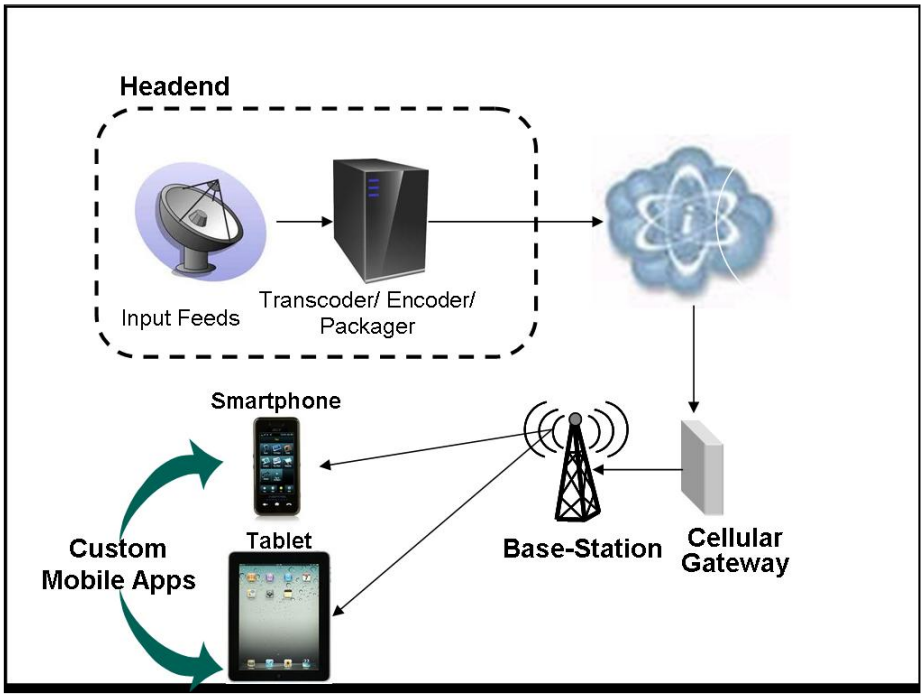

Figure 29: Broadband Alerting – Alerts via cable providers custom mobile apps.

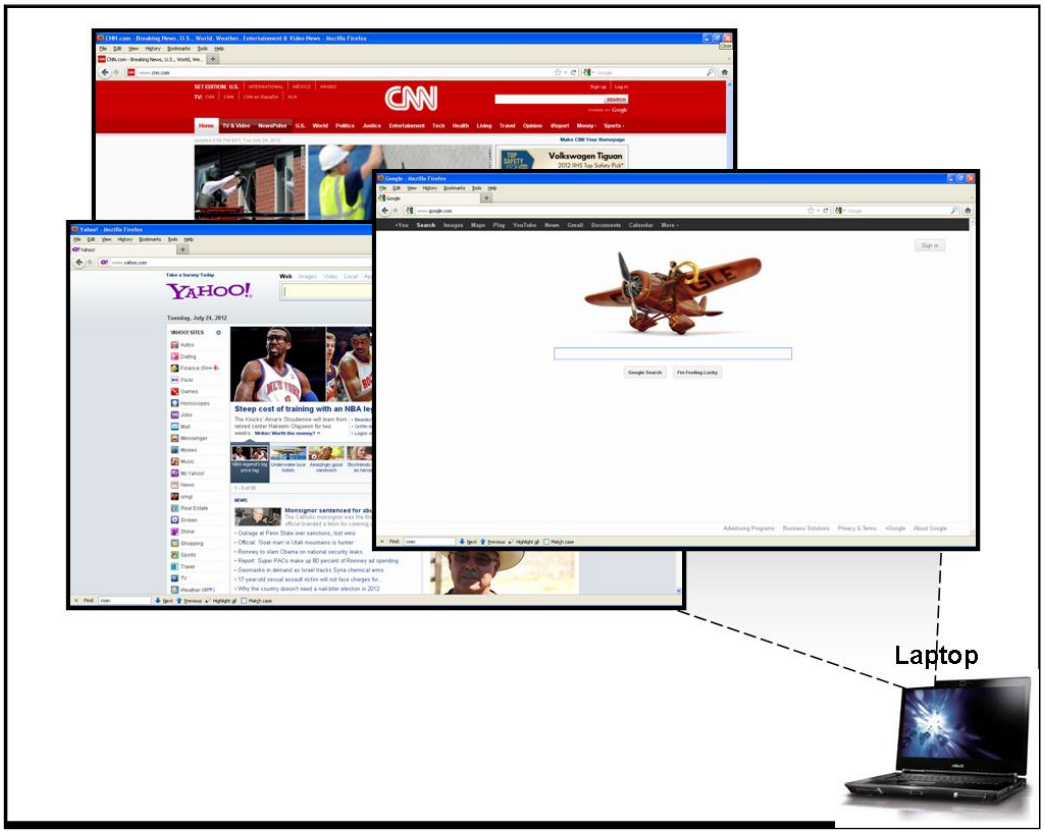

Figure 30: Broadband Alerting – Alerts via popular websites.

Figure 31: Broadband Alerting – Alerts via popular streaming media sources including "Over-The-Top" content.

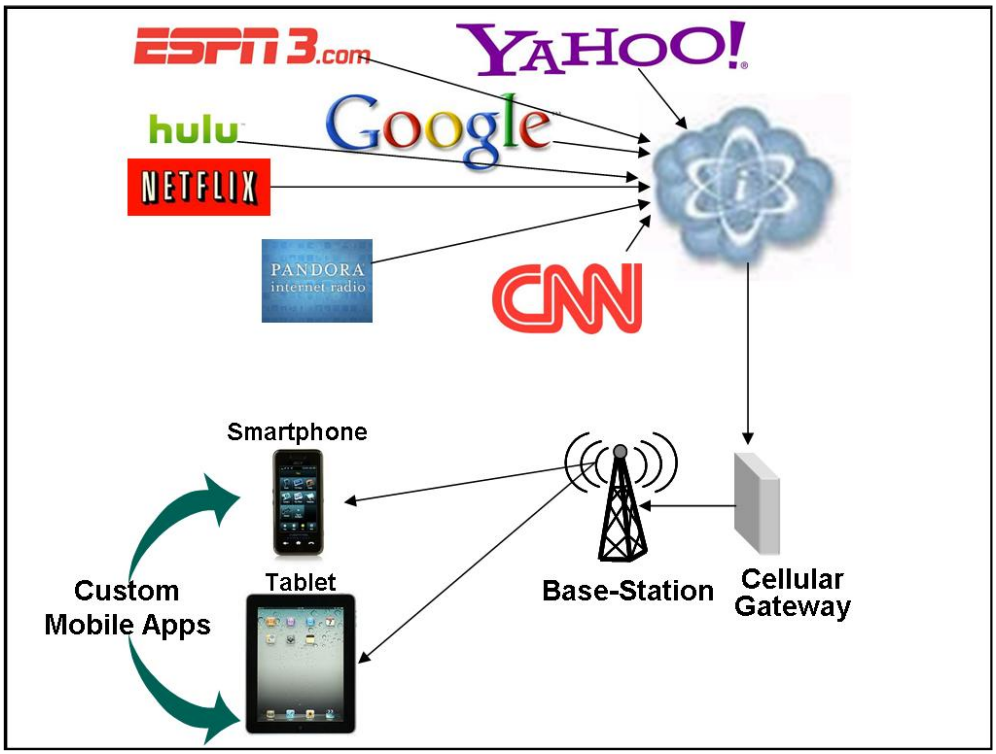

Figure 32: Broadband Alerting – Alerts via popular streaming media sources and/or websites delivered using custom Mobile apps.