March 2013
CAP Implementation

WORKING GROUP 9

Final Report – Part 4 March 2013

Table of Contents

This space left intentionally blank

1 Results in Brief

1.1 Emergency Alert System

The Emergency Alert System is the primary warning system that provides the President with the means to address the nation during a national crisis. Over the years it has gone through several transformations but until recently can best be described as an analog delivery system. On May 31, 2007, the FCC adopted a Second Report & Order (R & O) to strengthen the development of next generation technology for the Emergency Alert System (EAS)[1]. This R&O requires EAS participants to accept messages using Common Alerting Protocol (CAP) digital delivery.

Subsequently, on November 18, 2010 the FCC adopted the Fourth Report & Order to establish the deadline for EAS participants to start receiving CAP messages no later than June 30, 2012[2].

On January 10, 2012 the FCC released the Fifth Report and Order which further clarified the process to receive and transmit CAP messages for the EAS and to streamline the Part 11 rules[3]. CSRIC Working Group 9 was established to provide recommendations and best practice for the deployment of CAP and to provide an overall progress report on the first months of CAP implementation.

1.2 Executive Summary

As the Emergency Alert System (EAS) community adds an additional layer – supplementing the legacy broadcast based alerting relay platform with Common Alerting Protocol (CAP)-based platforms, there is a need for common deployment plans and best practices to help assist with the transition. The Working Group researched a number of architectural issue areas, and formulated several recommendations to CSRIC for EAS participants intended to facilitate their CAP migration processes. More importantly, the Working Group has identified a significant number of issues that we feel require additional examination.

1. The working group has a general consensus that the government should undertake testing and if necessary further development of a CAP Emergency Action Notification EAN streaming audio message capability.

2. The WG strongly advises that the existing EAS audio (radio) relay based on the Primary Entry Point (PEP) system **should remain in place as a required parallel system**, and continue to operate in order to provide a reliable, redundant pathway for Federal-level emergency messaging through broadcast media, in the event of a national emergency.

3. The working group recommends that the FCC coordinate with the Integrated Public Alert and Warning System, IPAWS, to ensure that proper Conformity Assessment support is provided, in the event that a manufacturer requires a test or re-test of a product.

4. The working group recommends that compliance with both a future streaming requirement, as well as the current IPAWS atom interface should be required for all CAP EAS devices.

[1] FCC Second Report and Order, in the Matter of the Review of the Emergency Alert System, EB Docket No. 04-296, Adopted: May 31, 2007
[2] FCC Fourth Report and Order, in the Matter of the Review of the Emergency Alert System, EB Docket No. 04-296, Adopted: September 15, 2011
[3] FCC Fifth Report and Order, in the Matter of the Review of the Emergency Alert System, EB Docket No. 04-296, Adopted: January 9, 2012

2 Introduction

CSRIC was established 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
- Resiliency of communications systems
  Including:
  - Telecommunications
  - Media
  - Public safety communications systems

Due to the large scope of the CSRIC mandate, the committee then divided into a set of Working Groups, each of which was designed to address individual issue areas. In total, 11 different Working Groups were created, including Working Group 9 on EAS CAP Implementation.

Working Group 9 officially started its work in December 2011 and was given until March 2012 to produce this First Report. The focus for Working Group 9 is to:

- Review the Fifth R&O (released January 10, 2012) on CAP deployment
- Provide FCC recommendations for best practices to facilitate CAP implementation on national, state and local levels
- Identify technological challenges.

The second report, presented in June 2012, reviewed audio format and authentication. In September 2012 the group reported on case studies from state and local implementation as well as best practices for message origination. Finally in March 2013 the working group will submit the final report on implementation.

2.1 CSRIC Structure

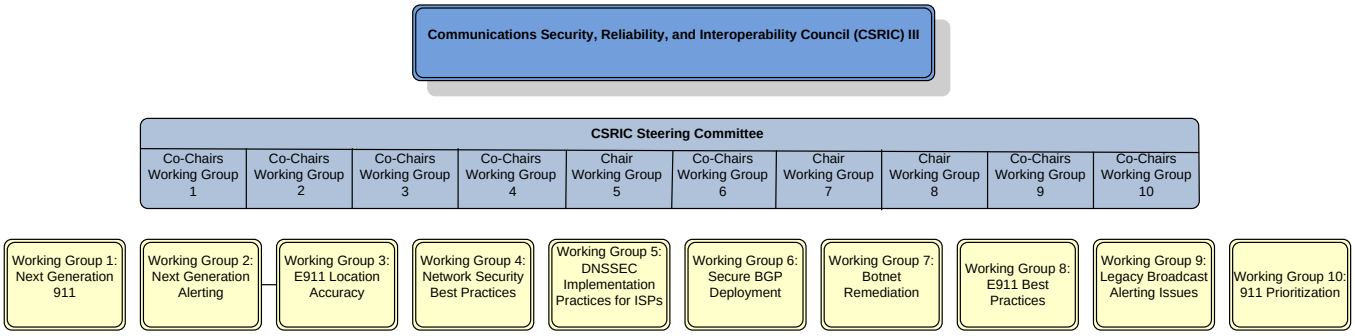


Figure 1 - CSRIC Structure

2.2 Working Group 9 Team Members

Working Group 9 consists of the following members:

Name	Company
Al Kenyon	Federal Emergency Management Agency (FEMA)
Andy Scott	NCTA
Arthur Leisey	EAS Consultant
Bill Robertson	Digital Alert Systems (Monroe Electronics, Inc.)
Bill Schully	DIRECTV
Bob Sherry	Intrado
Chris Homer (Chair)	DIRECTV
Clay Freinwald	Washington SECC
Daryl Parker	TFT
Donald Walker	GRM
Edward Czarnecki (Co-Chair)	Monroe Electronics, Inc.
Doug Semon	Time Warner
Gary Timm	Wisconsin SECC
Harold Price	Sage Alerting Systems
Herb White	NWS
Jared Maynard	Comlabs
Jeb Benedict	CenturyLink
Jeff Staigh	Univision
Jim Gorman	Gorman-Redlich
Kelly Williams	National Association of Broadcasters
Larry Estlack	Michigan Association of Broadcasters
Matthew Straeb	GSS
Michael Hooker	T Mobile
Mike Nawrocki	Verizon
Ron Boyer	Boyer Broadband
Tim Dunn	T Mobile
Eric Ehrenreich	FCC Liaison

Table 1 - List of Working Group Numbers

3 Objective Scope and Methodology

3.1 Objective

In its January 2012 EAS Fifth Report and Order (EB Docket No. 04-296), the Commission sought to continue the process to transform the Emergency Alert System (EAS) into a more technologically advanced alerting system by revising Part 11 Emergency Alert System (rules) to specify the manner in which EAS Participants must be able to receive alert messages formatted in the Common Alerting Protocol (CAP) and streamlining Part 11 rules to enhance their effectiveness and provide clarity.

The Fifth Report and Order is the second of two orders that implement Part 11 rule changes stemming from the Third Further Notice of Proposed Rule Making (FNPRM). The previous order, Fourth Report and Order, addresses the single issue of establishing a new deadline of June 30, 2012 for meeting the various CAP-related requirements that the Fifth R&O codifies. The Working Group was asked to review the new order to provide insight, implementation recommendations and status. In this Fifth R&O Report, the Working Group shall also recommend actions the FCC could take to improve EAS as it incorporates the new CAP protocol.

3.2 Scope

Per the Working Group 9 charter, the group found it essential to begin with an initial focus on the FCC Part 11 Rules governing the EAS as it involves best practices to facilitate CAP implementation leading up to and beyond the June 30, 2012 deadline. The committee will be working with real-time data and events as they unfold during the roll out. Based on results of these events the group will gain valuable insight and metrics that will be used for future planning and rulemaking.

3.3 Methodology

The Working Group 9 uses a collaborative, inclusive approach to its work. Given the array of expertise, the WG-9 members brought to bear on this effort, it is critical to provide a multitude of forums and mediums through which participants could express their opinions and help shape this Final Report. The following section details the methodology through which WG-9 achieved this objective.

3.3.1 Sub-Group Structure

After its initial set of meetings, the Chair and Co-Chair of Working Group 9 decided to review the structure of the Working Group and develop a plan that would allow for WG-9 to proceed with its study in an organized fashion which leveraged the diverse backgrounds of the Group's membership.

As such, WG-9 broke into two Sub-Groups; WG-9-1 is focusing on National implementation and best practices of CAP, WG 9-2 focusing on the progress of CAP implementation and best practices at the state and local level. The two Sub-Groups have moved forward with independent conference calls that focused almost exclusively on the portions of the CAP implementation most applicable to their expertise.

Each Sub-Group had a Lead who developed an agenda and framed conversation and discussion amongst the participants. On some of the more divisive issues, the Lead worked to bring members closer to consensus and encouraged open dialogue designed to find common ground.

3.3.2 Collaboration via Portal

In addition to the regular conference calls, an online collaboration portal was designed and implemented for use by the WG-9 participants. The portal is accessible to all Working Group members throughout the duration of their work on behalf of the CSRIC. Table 2 details some of the most prominent capabilities featured on the Portal and how they were used by the members of the Working Group 9.

Portal Capability	Description of Use
Document Repository	Collaboration space where members posted, reviewed, and edited documents
Forum	Open space where issues were discussed amongst members
Calendar	Central location where all relevant meetings and events were documented

Table 2

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 WG-9 members originated, having an online collaboration tool was instrumental to the successful completion of the Working Group's final product.

This space left intentionally blank

4 Background

From the onset of WG-9's work, close attention was paid to researching relevant topics, including the EAS, the Integrated Public Alert and Warning System (IPAWS), the CAP, and the Commercial Mobile Alert System (CMAS) and other alerting methodologies. Several members of the 9 Working Group brought specialized expertise in one or more of these areas and is also members of WG-2 that is focused on future developments in EAS systems.

4.1 Emergency Alert System (EAS)

EAS is the primary national warning system that provides the President with the means to address the nation during a national crisis. State and local officials also use EAS to originate warning messages about imminent or ongoing hazards in specific regions. Several Federal agencies share responsibility for EAS at the national level:

- FCC
- FEMA
- National Oceanic and Atmospheric Administration (NOAA) National Weather Service (NWS)

Functionally, EAS is a hierarchical alert message distribution system. Initiating an EAS message, whether at the national, state, or local level, requires the message originator (e.g. FEMA, which initiates EAS alerts at the national level on behalf of the President) to deliver specially-encoded messages to a broadcast station-based transmission network that, in turn, delivers the messages to individual broadcasters, cable operators, and other EAS Participants.

EAS Participants maintain special encoding and decoding equipment that can receive the message for retransmission to other EAS Participants and to end users (broadcast listeners, cable and other service subscribers).

4.1.1 Second Report and Order - Further Notice of Proposed Rulemaking

On May 31, 2007 the FCC adopted a Second Report and Order and Further Notice of Proposed Rulemaking (EB Docket 04-296, FCC-07-109A1) (Erratum, DA-07-4002A1) to strengthen the EAS and to promote the development of fully digital next generation technologies and delivery systems for EAS. The Second Report and Order requires EAS participants to accept messages formatted using CAP, the groundwork for next generation EAS delivery systems, no later than 180 days after FEMA announces its adoption of standards in each case. CAP is intended to ensure the efficient and rapid transmission of EAS alerts to the public in a variety of formats (e.g. text, audio and video) and via different channels (e.g. broadcast, cable, satellite, and other networks).

4.1.2 Third Further Notice of Proposed Rulemaking

On May 25, 2011, the FCC adopted the Third Further Notice of Proposed Rulemaking, in which they sought comment on a wide range of tentative conclusions and proposed revisions to the Part 11 rules that would more fully delineate and integrate into the Part 11 rules the CAP-related mandates adopted in the Second Report and Order. The Commission received 30 comments and 12 reply comments in response to the Third FNPRM.

4.1.3 Fourth Report and Order

Subsequently, on November 18, 2010, the FCC adopted the Fourth Report and Order in this docket, in which they amended section §11.56 of the EAS rules to require EAS Participants to be able to receive CAP formatted EAS alerts no later than June 30, 2012.

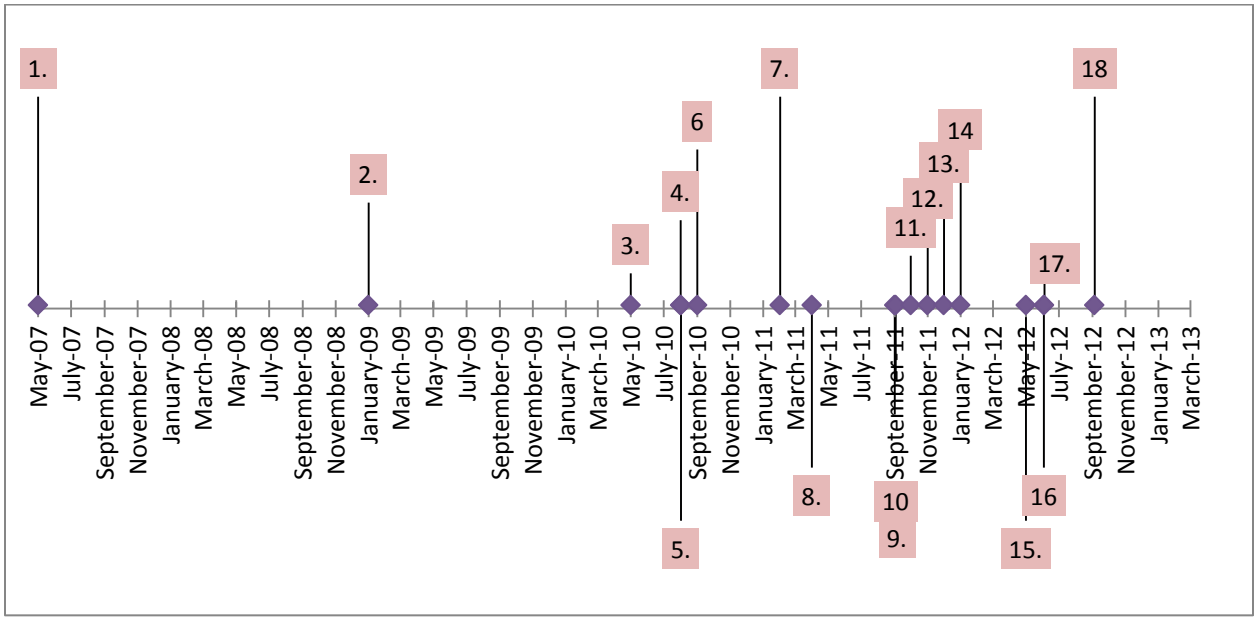
4.1.4 Fifth Report and Order

Finally, in the January 2012 FCC Fifth Report and Order on EAS (EB Docket No. 04-296), the Commission sought to continue the process to transform the Emergency Alert System (EAS) into a more technologically advanced alerting system by revising Part 11 Emergency Alert System (rules) to specify the manner in which EAS Participants must be able to receive alert messages formatted in the Common Alerting Protocol (CAP) and to streamline Part 11 rules to enhance their effectiveness and to provide clarity.

This section left intentionally blank

4.1.5 Chronological Highlights

DATE	MILESTONE	POSITION
May-07	FCC Issues 2nd Report & Order on Next Generation EAS - (First FCC action on CAP)	1
Jan-09	EAS CAP Industry Group (ECIG) Starts Work on Implementation Guide	2
May-10	ECIG Releases EAS-CAP Implementation Guide	3
Aug-10	Implementation of initial IPAWS-OPEN release v2.00	4
Aug-10	FEMA Memoranda Concurring with ECIG EAS CAP Guide	5
Sep-10	Adoption of IPAWS Profile v1.0/IPAWS CAP 1.2	6
Feb-11	FCC Issues Third Report & Order on EAS	7
Apr-11	First CAP EAS Devices Complete IPAWS Conformity Assessment	8
Sep-11	FCC Issues Fourth Report & Order on EAS (Extends CAP Compliance Deadline)	9
Sep-11	IPAWS-OPEN NOAA HazCollect Integration	10
Oct-11	IPAWS CAP EAS ATOM Feed Online	11
Nov-11	National EAS Test (no CAP)	12
Dec-11	IPAWS OPEN delivers first CAP messages for CAP/EAS devices	13
Jan-12	FCC Issues Fifth R&O on EAS (EAS rules revised)	14
May-12	First CAP EAS devices complete FCC CAP certification requirements	15
Jun-12	IPAWS-OPEN High Availability Standup/Testing	16
Jun-12	FCC Deadline to Have Ability to Receive CAP Alerts	17
Sep-12	Implementation of IPAWS Public Alert Feed	18



5 Analysis and Findings

5.1 Analysis and Findings

CSRIC WG9 is examining a broad range of questions relating to the usage of CAP for next-generation EAS;

5.1.1 CAP Distribution

1. What CAP-EAS Distribution Network architectures exist at the federal, state and local level?
2. What are the physical and data components of these systems?
3. What are the interface requirements

5.1.2 EAS Network Requirements

1. What is sufficient capacity to relay messages?
2. What availability is required to maintain service?
3. How does authentication work?
4. How is data security maintained? Data accuracy?

5.1.3 Findings Summary Table

Description	Finding	Recommendation
Network Architecture	Various (IP & Satellite)	Needs further study
Physical Components	Existing Technology	Industry Best Practices
Capacity Planning	Too early to evaluate	Needs further study
Availability	Too early to evaluate	Needs further study
Authentication	May not be sufficient	Needs further study
Security	Not available on all implementations	Needs Standardization
CAP EAN	Lack of specification	Testing of CAP EAN
FCC Equipment Certification	Ambiguous Ruling	Provide better clarity
EAS Message Duplication	Single event can generate multiple CAP/EAS messages	Implement Message ID

5.2 Findings CAP EAS Network Architectures and Platforms

As the Emergency Alert System (EAS) community adds an additional layer – supplementing the legacy broadcast based alerting relay platform with Common Alerting Protocol (CAP)-based platforms, there is a need for common deployment plans and best practices to help assist with the transition. The Working Group researched a number of architectural issue areas and formulated several recommendations to CSRIC for EAS participants intended to facilitate their CAP migration processes. Importantly, the Working Group has identified a significant number of issues that we feel require additional examination.

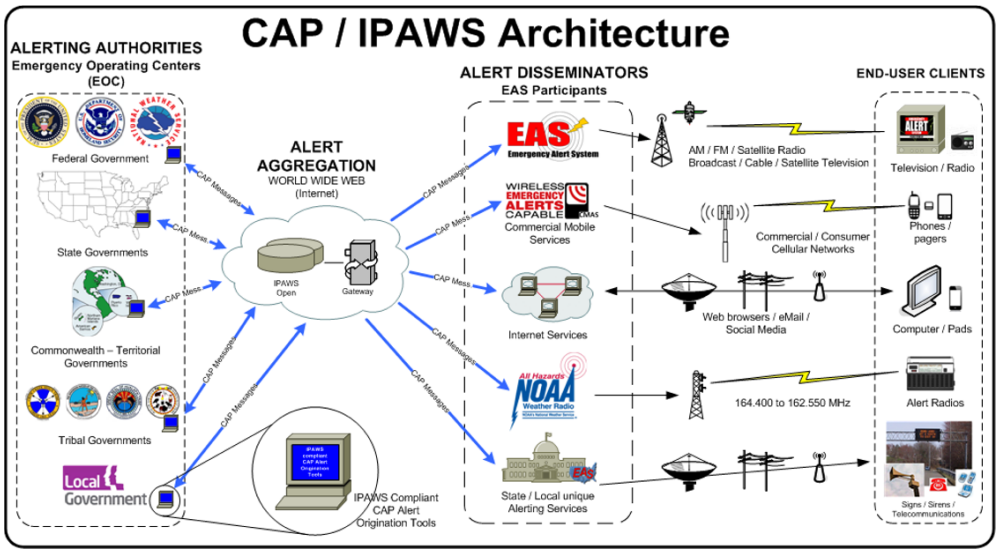
Therefore, the following information is principally intended to act as a guidepost to areas that require mor e in-depth study and policy discussion. It is important to stress that the following discussion is applicable to any IP-based CAP system. The Working Group is not associating our findings and recommendations with any single CAP system, whether Federal, state or local. The Working Group is, however, identifying a range of question areas that bear additional examination and scrutiny for any such public safety capabili ty.

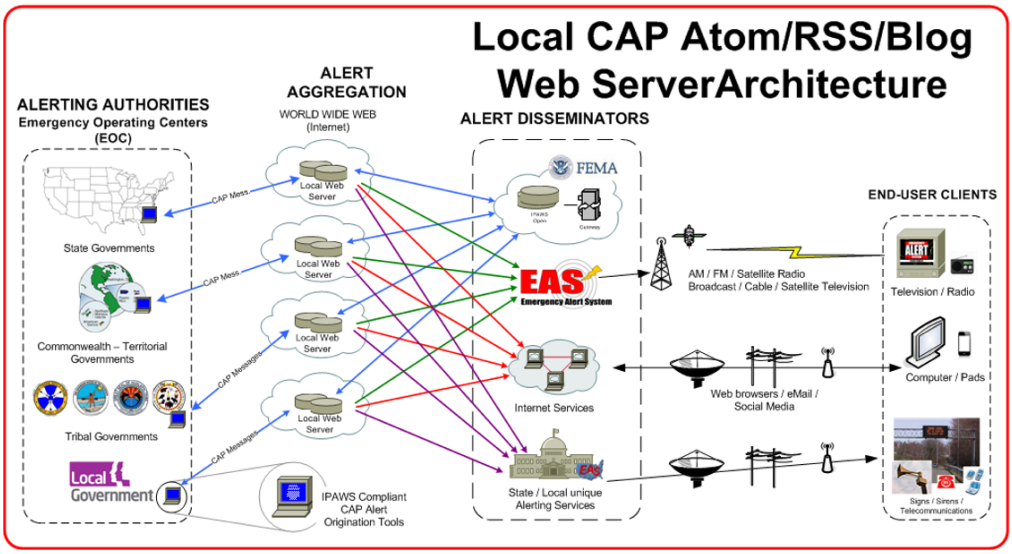
During this discovery exercise it became apparent that while general Best Practices and Network Standar ds exist in industry to provide guidance in the design, implementation and maintenance of any network th at may be considered necessary to facilitate the carriage of CAP alert messages, it was unclear which be st practices were adopted by CAP networks.

What also became evident was the lack of characterization of the CAP network operational requirements that are needed to assign, associate or designate the appropriate Best Practices and/or Standards. Base d on these basic conclusions, the following information is intended to note where additional studies are ne eded in order to fully understand what Best Practices and Standards are need to ensure an overall reliabl e network. The Key assumption that drives the following discussion is the “network is only as strong as its weakest link”.

The Working Group’s examination of CAP Architectures focused primarily on known means of web-based dissemination of CAP alerts for EAS activation. This focus was mainly driven by our understanding of the reliance of both the FEMA IPAWS system and a growing number of states, local and territorial CAP syste ms on web-based CAP dissemination. The Working Group is aware that various forms of satellite-based CAP dissemination are in use in a significant number of alert systems, principally at the state level. We d efer examination of satellite-based architectures for a future report.

Below, the next page shows both Federal (IPAWS) and state/local web-based CAP architectures. These are representations are intended to be archetypical, and not necessarily representative of any single extant CAP system.


CAP / IPAWS Architecture
ALERTING AUTHORITIES
Emergency Operating Centers (EOC)
Federal Government
State Governments
Commonwealth – Territorial Governments
Tribal Governments
Local Government
ALERT AGGREGATION
WORLD WIDE WEB (Internet)
IPAWS Open
Gateway
IPAWS Compliant CAP Alert Origination Tools
ALERT DISSEMINATORS
EAS Participants
EAS
Emergency Alert System
WIRELESS EMERGENCY ALERTS CAPABLE
Commercial Mobile Services
Internet Services
All Hazards NOAA Weather Radio
State / Local unique Alerting Services
END-USER CLIENTS
AM / FM / Satellite Radio Broadcast / Cable / Satellite Television
Commercial / Consumer Cellular Networks
Web browsers / eMail / Social Media
164.400 to 162.550 MHz
Television / Radio
Phones / pagers
Computer / Pads
Alert Radios
Signs / Sirens / Telecommunications


Local CAP Atom/RSS/Blog Web ServerArchitecture
ALERTING AUTHORITIES
Emergency Operating Centers (EOC)
State Governments
Commonwealth – Territorial Governments
Tribal Governments
Local Government
ALERT AGGREGATION
WORLD WIDE WEB (Internet)
Local Web Server
IPAWS Compliant CAP Alert Origination Tools
ALERT DISSEMINATORS
FEMA
EAS
Emergency Alert System
Internet Services
State / Local unique Alerting Services
END-USER CLIENTS
AM / FM / Satellite Radio Broadcast / Cable / Satellite Television
Web browsers / eMail / Social Media
Television / Radio
Computer / Pads
Signs / Sirens / Telecommunications

5.2.1 Overall Network

Reliability – The Working Group initially examined the question of what reliability requirements are being placed on this network, if any. For example is it to be considered a fully redundant and hardened network, are "five nines" reliability requirements necessary, or reasonable? The following table illustrates the requirements for each possible requirement.

Availability %	Designation	Downtime per year	Downtime per month*	Downtime per week
90.%	one nine	36.5 days	72 hours	16.8 hours
99.%	two nines	3.65 days	7.20 hours	1.68 hours
99.9%	three nines	8.76 hours	43.8 minutes	10.1 minutes
99.99%	four nines	52.56 minutes	4.32 minutes	1.01 minutes
99.999%	five nines	5.26 minutes	25.9 seconds	6.05 seconds

i. The choice of the above requirement will drive almost all of the basic design requirements through-out the entire network.
ii. The above requirement with also directly affect the cost of the overall network.
iii. It should be remembered that "all" elements of the network (end-to-end) must meet these requirements of the overall reliability will be impacted.
iv. Our initial suggestion is that achieving five nines of reliability and still using the Internet as the primary transport source will have not a significant impact on the overall network reliability.
v. At the same time, the actual delivery of information across the Internet cannot be regarded a high reliability or mission critical network. The Internet's current architecture uses a 'best efforts' delivery paradigm rather than a guaranteed end-to-end level of service. This factor was most often cited by critical infrastructure organizations as being the most significant reason why the Internet could not be relied upon for 'lifeline' applications.

5.2.2 Future of Internet Risks

Internet reliability risks are constantly evolving. Many fluctuations in the likelihood and consequence of various threats are expected to occur in the next ten years.

A table of expected movements in likely risks (**Like Trend**) and consequences (**Con. Trend**) is shown on the next page. (Green down=getting better, Red up=getting worse)

Category	Threat	Asset	Cause	Likely Risks (trend)	Consequences (trend)
Physical	Damage	Submarine Cable	Malicious	▪	↓
			Accidental	↓	↓
			Natural phenomena	▪	↓
		Terrestrial cable	Malicious	▪	↑
			Accidental	▪	↑
			Natural phenomena	▪	↑
		Telecommunications	Malicious	▪	↑
			Accidental	▪	↑
			Natural phenomena	▪	↑
		Satellite	Malicious	▪	▪
			Accidental	▪	▪
			Natural phenomena	▪	▪
	Failure	Submarine cable	Hardware fault	↓	↓
			Power interruption	▪	↓
		Terrestrial cable	Hardware fault	↓	↑
			Power interruption	▪	↑
		Telecommunications	Hardware fault	↓	↑
			Power interruption	▪	↑
		Satellite	Hardware fault	↓	▪
			Power interruption	▪	▪
	Interference	Transceivers	Weather	▪	▪

Electronic	Unauthorized use	Core routers	Compromise	▪	↑
			Misuse	▪	↑
		DNS infrastructure	Compromise	▪	↑
			Misuse	▪	↑
		Certification authority	Compromise	▪	↑
			Misuse	▪	↑
		Applications and protocols	Compromise	↑	↑
			Misuse	▪	↑
		End-user systems	Compromise	↓	↑
	Congestion	Capacity	Spam	▪	↑
			Worm	▪	↑
			Slashdot effect	▪	↑
			Denial of service attack	↓	↑
			Content size	▪	↑
			External failure affecting USA	▪	↑
		Quality of service	Spam	↓	↑
			Worm	↓	↑
			Slashdot effect	▪	↑
			Denial of service attack	↓	↑
			Content size	▪	↑
			External failure affecting USA	↓	↑
	Failure	Internet applications and systems	Software fault	▪	↑
			Misconfiguration	▪	↑

Other		Core routers	Misconfiguration	■	↑
			Routing loop	■	↑
	Interoperability issues	Interoperability	Protocol migration	■	↑
			Legacy Networks	↑	↑
	Service Closer	Infrastructure service	Business Issues	■	↑
			SLA Breach	■	↑
			Political	■	↑
	Loss of trust	Consumer confidence	Hijacking or theft	■	↑
			Ownership dispute	■	↑
	Unauthorized modification	Domain names	Hijacking or theft	↓	↑
			Ownership dispute	↓	↑
		IP addresses	Hijacking or theft	↓	↑
			Allocation dispute	↑	↑

5.2.3 Reasons for Network unavailability

In a study of Enterprise networks the following items were discovered to be the primary cause for network unavailability.

1. *Lack of best practices for change control*
2. *Lack of best practices for monitoring of the relevant components*
3. *Lack of best practices for requirements and procurement*
4. *Lack of best practices for overall operations*
5. *Lack of best practices for avoidance of network failures*
6. *Lack of best practices for avoidance of internal application failures*
7. *Lack of best practices for avoidance of external services that fail*
8. *Lack of best practices for physical environment*
9. *Lack of best practices for network redundancy*
10. *Lack of best practices for technical solutions for backup*
11. *Lack of best practice process solution of backup*
12. *Lack of best practices for physical location*
13. *Lack of best practices for infrastructure redundancy*
14. *Lack of best practices for storage architecture redundancy*

Security Considerations

1. As in assessing the reliability requirements, security has the same consideration that should be remembered. The surety of the end-to-end network is as good as the weakest link.
2. How should the network security requirements be classified? Is it considered a “life line” service or is it just a “data transport”?

5.2.4 Network Element-Alerting Authorities

As part of the Working Groups discussions, we observed the need for a set of best practices to guide both emergency managers and the systems development community in the process of CAP EAS message origination. While additional effort may be needed here to assist both emergency management and product developers, we assembled the following set of best practices as a starting point.

Cogestion	Capacity	Spam	—	▲
		Worm	—	▲
		Slashdot effect	—	▲
		Denial of service attack	▼	▲
		Content size	—	▲
		External failure affecting USA	—	▲
	Quality of service	Spam	▼	▲
		Worm	▼	▲
		Slashdot effect	—	▲
		Denial of service attack	▼	▲
		Content size	—	▲
		External failure affecting USA	▼	▲

Before you begin, complete the following:

1. Complete the FEMA IPAWS Basic Course IS-247.a
2. Message origination tool must comply with CAP 1.2 protocol, IPAWS 1.0 profile and ECIG implementation guide.
3. Have proper credentials and digital signatures for the CAP aggregator for which you are originating.
4. Review your particular State's FCC approved State Plan.

As we observed in currently requirements for Alerting Authorities there overall appears to be no common physical network security requirements established. Similarly, there does not appear to be any common criteria for data security.

1. The Working Group also find that there has been little consideration to of how to implement a "multimedia" server that would be needed to host audio files and other resource elements a Federal, state or local Alerting Authority may seek to make available to CAP EAS devices.

The Working Group similar found there has been little in the way of guidance to date for any potential requirements or specifications to support a multimedia or streaming server to support real-time live audio. The Working Group's observation was that this type of requirement would reasonably have been inferred to be a matter of compliance with the Presidential Order that the network be capable in carrying the EAN alert (Presidential Alert).

It is clear that both the FCC and many EAS participants expected the new CAP-based capability to support EAN messaging. The FCC's Fifth Report and Order on EAS states (paragraph 116) that the Commission "amending section 11.21 (a) to make clear that the State EAS Plans specify the monitoring assignments and the specific primary and backup path for SAME-formatted EANs and that the monitoring requirements for CAP-formatted EANs are set forth in section 11.52."

Section 11.52 (EAS code and Attention Signal Monitoring Requirements) requires EAS Participants to monitor FEMA's Integrated Public Alert and Warning System (IPAWS) for CAP EAN messages.

1. This issue ripples thru the entire network; it not only affects the alerting authorities, but the remaining elements of the network.

Security and reliability remain a concern as this origination point is neither reliable nor secure. The point of point of origin acts as a single point of failure, providing a very low reliability function, there by affecting the network's overall reliability.

1. Consideration should be given to allowing an interactive link between the point of origin and the end point (alert aggregator). Assuring that message delivery was achieved.

2. Depending on the characterization of the overall network reliability should be addressed. As it is now the reliability maybe less than 90% (one nine).

5.2.5 Network Element - Alert Aggregation / Distribution

Considerations for alert aggregation.

1. The details concerning this network are very limited. It has been stated that an internal effort of achieving five nines of reliability (99.999%) was being explored.
2. Even if five nines of reliability can be achieved within the alert aggregator that does not equate to an end-to-end system reliability achievement.
3. All stake holder parties involved with each network element must work together in order to achieve true end-to-end reliability.
4. Security is again a concern because so little is known as to the actual capabilities of the current alert aggregator. Whether this aggregator is local, state or Federal in nature, our recommendation is that "Best Practices and Standards must be both identified and universally utilized throughout the network.

5.2.6 Network Element - Alert Disseminators

These points of monitoring end points are:

1. EAS Participants including broadcast television
2. Broadcast radio
3. Cable television
4. IPTV
5. Direct broadcast satellite services.

With this wide array of monitoring points, maintaining a reliable and secure connection requires the FCC-mandated CAP devices need to be either an intelligent connection (connection aware) or a incorporate a secure transport (for example, VPN).

Within broadcast TV and radio, the monitoring end-point for CAP is effectively the broadcast facility. By comparison, cable and IPTV systems may push the CAP alert content to the set-top box in the customer premise itself.

It has been discovered that the hardware being used by the alert disseminators needs to support either internal or external security measures (firewall, etc.) in order to achieve overall network security.

We identified that one CAP EAS equipment manufacturer has published recommendations and best practices on securing the Alert Disseminator network element.[4] These best practices include the creation of a "defense in depth" strategy by EAS Participants that entails multiple layers of defense to prevent intrusions and attacks against critical systems. Defense in depth measures are intended to not only prevent security breaches, but also buy an organization time to detect and respond to an attack, thereby reducing and mitigating the consequences of a breach. We directly draw upon those published best practices with the below recommendations:

[4] "CAP, EAS and IPAWS: Introducing a defense-in-depth Security Strategy for Cable and IPTV Operations" (September 2011) Monroe Electronics.

Defense-in-depth involves using a number of layers. There are a number of options that EAS Participants, including the addition of a strong firewall and intrusion protection system in front of the CAP EAS equipment, creation of a DMZ, and use of a reverse proxy server within a DMZ. There are many additional options that should we have not discussed in the confines of this paper, such as network address translation (NAT), and adding additional obscurity.

The firewall is a first layer of defense; the proxy may be the second; using NAT, a third; obscuring the type of system adds another layer of defense. The Working Group concurs with the overall recommendations and best practices of a defense-in-depth strategy to defend the networks and infrastructure of EAS Participants, as identified in the EAS manufacturer's white paper:

1. Protect the local and wide area communications networks (e.g. from Denial of Service Attacks).Provide confidentiality and integrity protection for data transmitted over these networks (e.g. use encryption and traffic flow security measures to resist passive monitoring)
2. Defend the Enclave Boundaries (e.g. deploy Firewalls and Intrusion Detection to resist active network attacks)
3. Defend the Computing Environment (e.g. provide access controls on hosts and servers to resist insider, close-in, and distribution attacks).

However, we find that the lack of specific guidance or recommendations on security issues from government and alert dissemination sources to have been a significant area of oversight. The Working Group feels that it is critical that additional best practices and guidance be furnished to EAS Participants, from the FCC (or other agency), as well as from industry sources.

5.2.7 Network Element - EAS Clients

Both reliability and security are a concern to the EAS Participant, given that the edge device must attach the Internet and interface to their network. Security is a primary concern and therefore should be prioritized as such. At present there is minimal security implemented in the delivery path the EAS Participant.

Reliability should not be over-looked either at present there is no effective method to insure that an alert is received by the EAS Participant. At present the EAS participant must pull (request) the message from the Alert Aggregator. If the request is interrupted the EAS Participant must wait another polling cycle before trying again.

5.3 Findings and Observations

a) The current design of the CAP architecture was meant to utilize as many legacy EAS participant devices as possible. This may have precluded the optimal design criteria for network reliability and security.

b) The WG has a general consensus that the government should undertake the ability to initiate CAP EAN in order to properly address the regulatory requirements on EAS participants established under the Fifth Report and Order.

c) The WG strongly advises that the legacy EAS system should remain in place as a required parallel system, and continue to operate in order to provide a reliable, redundant pathway for Federal-level emergency messaging through broadcast media, in the event of a national emergency.

d) The WG agreed that there needs to be a generally known, published and identifiable requirements and timeline for implementing a CAP EAN that all stakeholders can organize around (including government, EAS Participants, EAS manufacturers).

e) The WG also noted all stakeholder need to be involved in the CAP EAN design process in some form, and that the government should take proactive efforts to coordinate with stakeholders. These stakeholders include:

6. EAS device manufacturers – to ensure compatibility with government design choices, and the CAP EAS equipment that has previously been installed since June 30, 2012.

7. EAS participants – to ensure they are properly informed of bandwidth and connectivity requirements to support a CAP EAN audio stream (compared with a basic IPAWS CAP XML file).

8. Federal agencies – principally DHS FEMA, the FCC and the National Weather Service, to ensure that all parties coordinate on the capabilities to be developed, and the timeline under which they would be deployed.

f) The WG observed that there would likely be a need for related standards/profiles to be updated (i.e. the ECIG Implementation Guide and potentially the IPAWS Profile).

g) Efforts must be undertaken to effectively synchronize the messaging between the radio-based PEP and IP-based CAP dissemination systems, including facilitating detection of message duplication.

h) The WG also observed that FCC will need to coordinate with EAS participants, to understand any added requirements a CAP EAN capability will entail (such as any additional IP bandwidth connectivity requirements, etc.).

5.4 Findings (State and Local)

5.4.1 State and Local EAS CAP Implementation

State and local governments have made great strides in implementation of CAP alerting. The Working Group reviewed four distinct case studies in report dated June 2012 of state and local CAP architectures, representing a diversity of technical approaches, using different background technologies. (See appendix)

There have also been a variety of approaches used for implementation. Some state and local governments have taken a top down approach (Washington State) while others have taken more of a grass roots approach (Michigan). (See appendix)

5.4.2 Distribution Network Architectures

There was also distinct difference in CAP EAS distribution network architectures – with some systems relying on internet dissemination, others relying on satellite dissemination, and another system using satellite and Internet in tandem.

5.4.3 Service Model Differences

There are also service model differences, one would encompass being “hosted by a third party” or an in-house deployed network server model.

5.4.4 Additional Differences

We observed additional differences in approaches to authentication and security among these case studies. While one system may rely on usage of the IPAWS digital signature credentialing for their own message authentication, another may incorporate both end-to-end encryption and authentication measures, while another may rely on simple posting of CAP messages on a webpage or RSS feed. While all four case studies cite interoperability with the FEMA IPAWS system, utilization of IPAWS by these different systems range from reference to the FEMA system as a redundant backup path, to reliance on IPAWS as a primary means of dissemination.

5.4.5 Early Adoption

Finally, early adoption was a key challenge for many states. Many protocols including CAP itself was in an infantile state and required further development for the implementers. Also funding and support may be scarce and there may not be enough trained individuals to provide operations and technical support.

5.4.6 Looking Ahead

Many questions arise when looking ahead for state and local. There are currently new delivery methods for broadcasters including:

1. ATSC Mobile
2. HD Radio
3. Radio Data System
4. RDS
5. Text of which nearly 80% of FM radio broadcasters support.

How do these new delivery opportunities for broadcasters work with legacy and CAP alerts?

With increase adaption of CAP will create an ability to provide emergency alerting access for entities such as schools and universities, municipalities, local law enforcement which previously did not exist.

There will need to be both awareness and outreach to the public on CAP/EAS so expectations can be properly managed. In addition much needed training to get operating personnel up to speed on new systems will need to occur in the future and best practices will need to be established. This could create broader liability and burden on existing local budgets.

With regard to EAS messages these new entities will need to work closely with state and local State Emergency Communication Committees (SECC) and Local Emergency Communication Committees (LECC).

This space left intentionally blank

6 Recommendations

6.1 The Emergency Action Notification [EAN] and CAP

6.1.1 Expectations of a CAP EAN

47 CFR Part 11 contains rules and regulations addressing the nation's Emergency Alert System (EAS). The EAS provides the President with the capability to provide immediate communications and information to the general public at the national, state and local area level during periods of national emergency. This capability is typified in the Emergency Action Notification (EAN) event code. The EAN alert is unique among all other EAS codes in several respects:

- The EAN provides the originator with audio messaging length of unlimited duration (all other EAS event codes are limited to two minute duration).
- The EAN alert must be carried at any time, and cannot be "filtered" out by the EAS participant.

The EAS also provides state and local governments and the National Weather Service with the capability to provide immediate communications and information to the general public concerning emergency situations posing a threat to life and property. Regardless, a primary role for the EAS system is the dissemination of the Emergency Action Notification.

It is clear that both the FCC and many EAS participants expected the new CAP-based capability to support EAN messaging. The FCC's Fifth Report and Order on EAS states (paragraph 116) that the Commission "amending section 11.21 (a) to make clear that the State EAS Plans specify the monitoring assignments and the specific primary and backup path for SAME-formatted EANs and that the monitoring requirements for CAP-formatted EANs are set forth in section 11.52."

Section 11.52 (*EAS code and Attention Signal Monitoring Requirements*) requires EAS Participants to monitor FEMA's Integrated Public Alert and Warning System (IPAWS) for CAP EAN messages.

The EAS CAP Implementation Guidelines, which were formally adopted by the FCC alongside the IPAWS CAP profile and Common Alerting Protocol.

6.1.2 Constructing EAS Streaming Audio from CAP V1.2 IPAWS v1.0 Profile

Where a streaming audio message intended for EAS use accompanies the CAP message in a CAP <resource> block, such as for an EAS EAN message, the EAS streaming audio message is constructed as follows:

1. As required by the IPAWS profile, the CAP <resourceDesc> element value SHALL be "EAS Broadcast Content."

2. The audio SHALL use one of the following streaming methods:
    a. MP3 streaming as either HTTP progressive-download streaming, or
    b. HTTP streaming MP3 server.

Further, the ECIG guidelines also provide a hypothetical example of a CAP EAN message (see Section 5.3, ECIG Guidelines). That example points to how the audio resource can have a very important difference in a National Alert.

"The EAN and EAT National alerts are designed to broadcast live (they can of course still be pre-recorded audio) from the White House to the American public. A CAP alert can reference a slightly delayed, progressively downloaded live audio stream carrying this alert message.

The audio stream SHOULD be able to start from the beginning in order that none of the important message is lost. The example shows how an audio resource could be constructed to provide this reference"

6.1.3 CAP EAN Streamed Audio Message for IPAWS OPEN

The IPAWS architectural design supporting a CAP-based EAN alert streamed audio message has yet to be tested. Informal conversations with IPAWS staff have indicated that a CAP EAN streamed audio message capability is supported.

However, to date, the government has not provided any additional specifications for a CAP-based EAN, including audio stream requirements other than to state that the OPEN design is compatible with the ECIG guidelines.

As noted in the ECIG recommendations, the unique nature of an EAN message would not rely on text to speech capability, and would require usage of either downloaded audio file resource, or access to a "live" IP audio stream. Both resources would ostensibly be sought by the CAP EAS device from a third party server or media resource, defined within the CAP message.

The lack of a tested EAN streaming audio message capability over CAP appears to be highly problematic from a technical, operational and regulatory perspective. From a technical and operational perspective, all EAS Participants were to have procured, installed and have operating their FCC-compliant CAP EAS equipment by or before 30 June 2012. To the working group's understanding, EAS Participants have to a great extent worked to comply with that regulatory mandate.

However, this CAP EAS equipment was designed and furnished to the CAP and EAS specifications that were available at that point in time. Therefore, tens of thousands of CAP EAS units have already been deployed throughout the nation, and any changes in specifications to accommodate a streaming CAP-based EAN would impact this previously installed equipment. While most of this CAP EAS equipment appears to be software or firmware upgradeable, the issuance of any new specification would appear to place the burden on the specification developer (the government) to provide a specification that is compatible with any software and hardware limitations in this previously-installed equipment.

It appears that much of the rationale for the adoption of CAP by the FCC, and the regulatory requirement for EAS participants to implement upgraded CAP EAS capabilities had been based upon the existence of a CAP EAN message in addition to a conventional radio-based EAS CAP message. The conventional broadcast EAN (via the Primary Entry Point system) provides a highly resilient capability for EAN dissemination. This is crucial particularly in light of circumstances which might surround actual usage of a national Emergency Action Notification. However, the regulatory requirements for a CAP EAN (including the issue that CAP EAS was in part predicated on the existence of a CAP EAN), infers that the omission of a CAP-based EAN capability operating in parallel with the broadcast EAS-based EAN is a situation that needs to be rectified in the very near term.

6.1.4 Recommendation

1. The working group has a general consensus that the government should undertake testing and if necessary further development of a CAP EAN streaming audio message capability. We feel that such testing of a CAP EAN streaming audio message capability proceed with all deliberate speed, in order to properly address the regulatory requirements on EAS participants established under the Fifth Report and Order.

2. The WG strongly advises that the existing EAS audio (radio) relay based on the Primary Entry Point (PEP) system **should remain in place as a required parallel system**, and continue to operate in order to provide a reliable, redundant pathway for Federal-level emergency messaging through broadcast media, in the event of a national emergency.

3. The WG agreed that there needs to be a generally known, published and identifiable requirements and timeline for implementing a CAP EAN that all stakeholders can organize around (including government, EAS Participants, EAS manufacturers).

4. The WG also noted all stakeholder need to be involved in the CAP EAN design process in some form, and that the government should take proactive efforts to coordinate with stakeholders. These stakeholders include:

    i. EAS manufacturers – to ensure compatibility with government design choices, and the CAP EAS equipment that has previously been installed since June 30, 2012.

    ii. EAS participants – to ensure they are properly informed of bandwidth and connectivity requirements to support a CAP EAN audio stream (compared with a basic IPAWS CAP XML file).

    iii. Federal agencies – principally DHS FEMA, the FCC and the National Weather Service, to ensure that all parties coordinate on the capabilities to be developed, and the timeline under which they would be deployed.

5. The WG observed that there would likely be a need for related standards/profiles to be updated (i.e. the ECIG Implementation Guide and potentially the IPAWS Profile.

6. Efforts must be undertaken to effectively synchronize the messaging between the radio-based PEP and IP-based CAP dissemination systems, including facilitating detection of message duplication.

7. The WG also observed that FCC will need to coordinate with EAS participants, to understand any added requirements a CAP EAN capability will entail (such as any additional IP bandwidth connectivity requirements, etc.).

6.2 FCC Equipment Certification Issues

6.2.1 Potential Impact of Future Spec Changes on Existing FCC-Certified CAP EAS Equipment

As CAP requirements evolve in the future, and as CAP EAS equipment manufacturers offer improvements and enhancements to their products, the working group discussed the potential for such a change to impact the FCC certification requirements surrounding such equipment, as well as the potential need for re-testing under related programs, such as the IPAWS Conformity Assessment Program. (The permissive change rules in Section 2.1043 describe the modifications that may be made to an RF device without filing for a new equipment authorization; define the three different types of permissive changes; and identify when a permissive change (PC) filing with the Commission is required).

Part of the difficulty in clearly identifying what types of changes would require a permissive change filling – or even re-certification – may stem from the issue that CAP EAS equipment are not strictly RF devices (per se), though they are required to follow the same certification processes of RF equipment.

The understanding of the working group is that when a government-certified device is modified, all proposed changes must be considered to determine the type of change filing required. For example, a software/firmware change to add support for streaming media capabilities (for CAP EAN message) could very conceivably require authorization by a “permissive change” filing.

Because of the CAP EAS equipment certification requirements set forth by the FCC, equipment of this type was required to furnish a Suppliers Declaration of Conformity (processed though the IPAWS Conformity Testing Program), or similar Test Report.

Further, a change in CAP, IPAWS or ECIG specifications would appropriately seem to require some form of re-testing under the IPAWS Conformity Assessment Program (as the program itself asserted that any significant changes to the products after initial testing would require resubmission to the testing process – though it appears to be left to the manufacturer to determine what a significant change might be).

6.2.2 Issues Related to FCC Certification Process

Because of FCC guidance on certifying CAP EAS equipment appears primarily focused on the initial certification of CAP compliance, the working group felt that the FCC should provide additional guidance to the manufacturing community as to what types of changes may (or may not) trigger a permissive change filing, a CAP conformity re-testing, and/or re-certification.

6.2.3 Issues Related to IPAWS Conformity Assessment Program

A related issue is that of how the FCC CAP EAS certification process and IPAWS Conformity Assessment process interrelate. FCC CAP EAS certification relies in large part upon the existence of a Suppliers Declaration of Conformity (as processed through the IPAWS CA testing process). However, that Declaration of Conformity references specific software versions and software-hardware combinations.

What types of changes to software are permissible without requiring either an IPAWS conformity retest or permissive change filing? What material changes would necessitate a retest or filing? If a manufacturer even changes its software version (as specifically referenced in the SDoC and Test Report), does it technically risk its FCC CAP EAS certification?

6.2.4 Issues Related to Future Testing

Finally, testing of CAP EAS equipment's ability to physically access the IPAWS server was not part of the original conformance tests. Such verification was also not part of the Class II permissive change filing required by the Fifth Report & Order. Compliance with a transport specification (such as the IPAWS RSS ATOM feed) has so far not been a part of either formal Part 11 certification testing or the IPAWS Conformity Assessments. This may be a major oversight in the equipment certification regime, one that may present additional problems should additional transport and signaling requirements be added in the future.

6.2.5 CSRIC WG 9 Recommendations

1. The working group recommends that the FCC provide additional clarification and guidance for the manufacturing community as to what product (and specifically software) modifications may require a permissive change filing, conformity retest, recertification, or no action required on the part of the manufacturer.

2. The working group recommends that the FCC coordinate with IPAWS to ensure that the P-TAC Center continue providing CAP 1.2 USA IPAWS Profile 1.0 message conformance testing with no-cost to the test or creating the report until the technology is mature or another suitable testing unit is available.

3. The working group recommends that a check for conformance to the IPAWS-OPEN transport interface (currently Atom) be added to the P-TAC test, and that a check for conformance to the EAN streaming format be added once it is defined by FEMA.

This space left intentionally blank

6.3 EAS Duplicate Message Handling

6.3.1 Summary

- Discuss ongoing need for EAS
- Discuss causes of the problem
- Mention that CAP makes it worse
- Introduce concept of message id
- Discuss how to add message id to existing EAS protocol that is minimally invasive and transparent to legacy devices

6.3.2 Finding

The nationwide Emergency Alert System (EAS) provides an effective and efficient method of public alert message dissemination by leveraging a large network of radio, television, cable and satellite television operators to achieve a robust and redundant method of conveying messages to the listening and viewing public. Moreover, while sometimes referred to as "legacy EAS" its broadcast roots remain the most effective communication method when other land-based or wired communication infrastructures may have collapsed.

In addition the number of broadcast users is unrestricted and unrestrained offering the most economical means to reach a mass audience – regardless of audience size.

To help assure message delivery EAS participants monitor at least two, and in some cases, more, sources of FSK audio EAS messages. Messages are originated or relayed by one or more of these monitored sources, thereby EAS participants may receive the same message multiple times. As such, the detection of duplicate messages is an essential part of the EAS system. By properly detecting and handling duplicate EAS messages a broadcast station or cable operator is prevented from sending the same message multiple times.

An EAS device stores recently received messages and compares each newly received message to the stored copies. A byte-by-byte comparison is done for each message. The message elements compared include the three-byte originator code, the three-byte event code, list of locations codes, the start time, and the duration[5]. Messages that match are duplicates, and all but the first received version are ignored.

This duplicate detection method works as intended, weeding out expected duplicate EAS messages if multiple stations relay each alert. However, it falls short, when the same audio portion of the message (audio payload) is included in multiple, non-duplicate, EAS messages. While this may sound obvious the resultant audio payload repetition is the problem because, if any one or more of the message comparison elements are different, the message is NOT considered the same emergency alert – although it may contain the same audio message. Since the EAS device sees different data elements, it can transmit multiple copies of what appears to the public as the same information.

This unfortunate aspect of EAS has always been present, but is rarely seen mainly due to geographical boundaries. Moreover, since retransmission of most EAS message(s) is voluntary, extra interruptions for the same information leads to audience fatigue (a kind of "cry wolf" syndrome), wasted airtime, and unhappy station owners.

[5] The call sign of each relay point is not included in the comparison.

Duplicate messages are mainly caused by two cases:

1 The National Weather Service (NWS) transmits information regarding a large storm over multiple NOAA transmitters, using a different, but overlapping, list of location codes on each transmitter.
2 Two different civil authorities issue a message, typically a required monthly test, with an overlapping set of location codes, on different transmitters.

For example, assume a large storm system causes the NWS to issue an alert over multiple NOAA transmitters. Each transmitter sends the message to the location codes in its coverage area. For example, NOAA transmitter number one sends the message to counties A, B, and C. NOAA transmitter number two sends the message to counties C, D, and E. The problem is the two transmitters send two messages covering county C. Since they have different location lists the messages are *not considered* duplicate EAS messages, therefore a station in county C could relay both messages even though the audio payload is identical.

In the past, most stations have been protected against this source of message duplication because natural RF barriers kept the messages from multiple origination points from being widely distributed forming a “geographic shield”. Also, receiving stations rarely monitor two NOAA transmitters, or an EAS relay point that would have relayed both messages.

In some parts of the country, however, the problem can, and does, occur as in the civil case, alerts to boundary regions, typically in large counties or along state borders, civil authorities on either side of the region will sometimes use overlapping location lists. However, with EAS messages disseminated to all EAS Participants via the FEMA's IPAWS CAP feed the geographic shield is removed. Every station can “hear” both the original CAP alert and the version transmitted by their local NOAA transmitter. If the NOAA transmitter sends a subset of the full location list in the CAP message to EAS, unintentional EAS duplicates have been generated. Both versions could be aired by broadcast stations and cable head-ends.

This is a general problem - any time a single CAP message can generate more than one EAS message, undetectable duplicates in the EAS domain have been created.

6.3.3 Recommendation

What is needed is a method for originators to tag EAS messages with additional data to allow newer or upgradable equipment a means to uniquely identify the source message and provide better duplicate message handling while simultaneously not creating problems for existing equipment.

CAP, with its larger set of data elements and greater bandwidth can easily solve the problem, but legacy EAS has much lower bandwidth and a very small set of data elements; moreover it cannot break existing equipment, or require substantial replacement.

Three problem Cases

1. The same source of information may be used to generate multiple CAP messages – possibly with different sent times.

2. The same CAP message is used to generate multiple EAS messages (e.g., the NWS case where an event covers more than 31 locations or more than 1 NOAA transmitter coverage area with different location lists).

3. Two different originators are sending the same information as an EAS message, either to different location lists, and/or with a different origination time stamp.

There is no clean way to take the existing EAS spec and disambiguate two alerts with the same originator, time, and event, duration, but overlapping lists of location codes. We can guess, and maybe get it right much of the time, but that's no way to run an essentially automated system.

One solution path is to add something to the spec that will provide a higher-level alert id, so that an EAS message with the same time, event, and originator, but a different set of location codes, but the same alert id, would be tagged as a duplicate. If the alert id is strong enough, possible to even loosen the constraint that the time stamp match and duration exactly - solving another NWS problem.

The intent for EAS is not to do a globally unique string like the CAP combination of sent, sender, and identifier elements - this way is too long. Even a 128 bit GUID is longer than needed. A number long enough to disambiguate the alerts issued that hour could suffice, 10 or 11 bits should suffice.

These can be encoded into two extra bytes. There are many ways to add this additional information, including;

1) Add a few bytes to the end of the ZCZC string, after the LLLLLL-. This should not confuse legacy devices as they stop listening after the last '-', it won't sound different to the ear, and should not confuse any other EAS device (like Radio Shack S.A.M.E receivers). It also delivers the alert id before any other switching action would occur in new EAS devices that are putting the alert on the air while it is still being received. It would require a change to NWS consoles (that part that generates the headers).

2) Add a trio of short headers after the attn tone. Might confuse some legacy devices that simply listen for any valid bytes to start a receive process. Could use different sync bytes to avoid that. It will sound different to the ear. Would require a change to NWS consoles.

3) Send the alert id as a location code. Pick an unused state code that would mean alert id, use the CCC part as the alert ID. This would not require a change to the generation of the ZCZC string at the NWS, just the addition of an otherwise bogus location code. Reduces total available for real locations to 30.

4) Add additional FSK data to the audio payload. These short “braps” would allow additional message ID information to be encoded as part of the specific message itself. By using a different preamble the data is ignored by legacy devices and is always passed without a problem.

The message will sound differently to an astute listener, but not so much as to be annoying due to the short nature of the “brap” and could be considered as part of the attention tones, and would require changes to the NWS audio message generation, but no changes to the actual EAS generator.

Following this method does not require modification of the current Part 11 coding structure and could be quickly adopted as an addendum to the current decoding practice by all EAS vendors. Also, using this method provides a more extensible means to encode any additional data that may be considered important in the future. While current thinking is the addition of two-bytes for a unique message ID is good, there may be a future need for more data and this method provides a much easier path to future expansion.

All of these require some action by NWS to provide the alert id, and an alert id parameter would need to be added to the CAP message for 1), 2) and 4). Any of these this would allow a much better method to determine which alerts are duplicates, even if the locations, and possible the time/duration, differ. It cannot by the EAS/CAP devices alone since additional data input is needed.

Any solution will need to be tested to; A) validate EAS duplicate messages are properly filtered and, B) ensure legacy EAS devices and legacy radio receivers, including those used as inputs to EAS devices and in consumer devices, are not adversely impacted by the solution. NOAA’s National Weather Service (NWS) encourages consumers purchase receivers that display the Public Alert logo indicating that it meets certain performance criteria including SAME decoding.

The NWS and others worked with the Consumer Electronic Association (CEA) to develop the *Receiver Performance Specification for Public Alert Receivers* (CEA-2009-B (ANSI)), a voluntary standard that defines minimum performance criteria for consumer electronic products designed to receive SAME alert signals. NWS Directive System 10-1712, *NOAA Weather Radio (NWR) Specific Area Message Encoding (SAME)*, describes the format and use of NWR SAME from which EAS SAME was derived.

6.4 Usability of CAP Message Text for Direct-to- Broadcast Use

6.4.1 Description of the Issue

As stated in the OASIS CAP standard:

> "CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task"[6]

The WG takes note, however, that different warning systems have different technical limitations and different audiences for the information. When using CAP to generate EAS messages, the CAP data is presented directly to a broad general public, audience. The contents of the description and instruction fields are used to:

1. Provide the text used for video crawls and page by page displays for TV and Cable.

2. Provide text used for radio-based text systems, such as the text capabilities of HD radio and RDS.

3. Provide the input for text to speech generators, either centrally located at a reply point, or in the end point CAP/EAS devices.

In all of these cases, there is no human processing of the data once it leaves the originator. Particularly in radio and cable; most radio stations and cable head-ends are unattended some of each day, and some stations and cable head-ends are unattended most of each day. There is no human the loop.

The following discussion is primarily based on the NWS use of CAP for EAS, because they have been, and will likely continue to be, the originator of the largest number of EAS-bound messages. The general observations and recommendations apply to all CAP messages intended for broadcast via EAS, not just NWS messages.

The WG is concerned that the text of CAP messages currently provided by the NWS may not suitable for direct use by the general public via the broadcast medium. NWS messages have been successfully used for many years by many people and automated processes, however, these users have always needed to make an effort to obtain the information, and are likely to be self-selected to know what they are looking for, and by experience, better understand what they get. Once NWS goes live on CAP/EAS, a new and different community of users will be involved, who won't be expecting the information and won't be as prepared to make allowances and assumptions about what they are getting.

In particular, we note the content of the messages includes abbreviations, time in a different standard format, email addresses, telephone numbers, web page addresses, use of upper case only, limited use of punctuation, and lengthy lists of locations.

Some messages are short, but may be hard to read as a video crawl, for example:

```
AT 1237 PM CST...NATIONAL WEATHER SERVICE DOPPLER RADAR INDICATED
A SEVERE THUNDERSTORM CAPABLE OF PRODUCING A TORNADO. THIS
```

[6] Common Alerting Protocol Version 1.2, OASIS Emergency Management Technical Committee, July , 2010, Page 1.

```
DANGEROUS STORM WAS LOCATED 5 MILES NORTHWEST OF SPRING HILL...OR
8 MILES NORTHEAST OF MIDWAY...MOVING NORTHEAST AT 60 MPH.
LOCATIONS IMPACTED INCLUDE... HURTSBORO...UCHEE...RUTHERFORD AND
HATCHECHUBBE. TAKE COVER NOW. MOVE TO AN INTERIOR ROOM ON THE
LOWEST FLOOR OF A STURDY BUILDING. AVOID WINDOWS. IF IN A MOBILE
HOME...A VEHICLE OR OUTDOORS...MOVE TO THE CLOSEST SUBSTANTIAL
SHELTER AND PROTECT YOURSELF FROM FLYING DEBRIS.
```

Without training, Text to Speech engines may interpret the text “AT 1237 PM CST” as a voice output of “at one thousand two hundred thirty seven”. Human readers or a video crawl will have trouble with all capital letters and the use of the “…” strings.

Some messages are far from usable for EAS broadcast. Although most EAS Operational Plans do not advocate broadcast of flood warnings (FLW), this recent flood warning highlights the issues in some messages intended for broadcast…

```
<description>...THE NATIONAL WEATHER SERVICE IN CORPUS CHRISTI HAS ISSUED A FLOOD
WARNING FOR THE FOLLOWING RIVERS IN TEXAS...   ARANSAS RIVER NEAR SKIDMORE AFFECTING
BEE ALL PERSONS WITH INTERESTS ALONG THE RIVER SHOULD MONITOR THE LATEST
FORECASTS...AND BE PREPARED TO TAKE NECESSARY PRECAUTIONS TO PROTECT LIFE AND
PROPERTY. RIVER STAGE FORECASTS ARE BASED ON OBSERVED AND PREDICTED RAINFALL. IF
ACTUAL RAINFALL VARIES FROM FORECAST VALUES...FORECAST RIVER STAGES WILL VARY
ACCORDINGLY. FOR THE LATEST RIVER STAGES AND FORECASTS VISIT OUR WEB PAGE AT
WWW.SRH.NOAA.GOV/CRP. IN THE BLUE MENU SECTION ON THE LEFT OF THE PAGE...UNDER THE
"CURRENT WEATHER" SUBMENU...CLICK ON "RIVERS/LAKES" WHICH TAKES YOU TO OUR AHPS WEB
PAGE.THE NATIONAL WEATHER SERVICE IN CORPUS CHRISTI HAS ISSUED A * FLOOD WARNING FOR
THE ARANSAS RIVER NEAR SKIDMORE.* UNTIL THURSDAY AFTERNOON...OR UNTIL THE WARNING IS
CANCELLED.* AT  7:15 PM WEDNESDAY THE STAGE WAS 13.1 FEET. * MINOR FLOODING IS
OCCURRING AND MINOR FLOODING IS FORECAST.* FLOOD STAGE IS 13.0 FEET. * FORECAST...THE
RIVER WILL STAY AROUND A CREST OF 13.1 FEET FOR THE NEXT SEVERAL HOURS AS A RESULT OF
HEAVY RAINFALL OVER THE PAST 24 HOURS. IT WILL FALL BELOW FLOOD STAGE LATER TONIGHT.*
FLOOD HISTORY...THIS CREST COMPARES TO A PREVIOUS CREST OF 13.3 FEET  ON NOV 21 2009.*
AT 13.0 FEET MINOR LOWLAND FLOODING OCCURS WHICH WILL COULD IMPACT A FEW RESIDENCES.
CROPS AND PASTURE LANDS ARE THREATENED.</description>

          <instruction>FOR THE LATEST RIVER STAGES AND FORECASTS VISIT OUR WEB PAGE AT
WWW.SRH.NOAA.GOV/CRP. IN THE BLUE MENU SECTION ON THE LEFT OF THE PAGE...UNDER THE
"CURRENT WEATHER" SUBMENU...CLICK ON "RIVERS/LAKES" WHICH TAKES YOU TO OUR AHPS WEB
PAGE. ALL PERSONS WITH INTERESTS ALONG THE RIVER SHOULD MONITOR THE LATEST
FORECASTS...AND BE PREPARED TO TAKE NECESSARY PRECAUTIONS TO PROTECT LIFE AND
PROPERTY. RIVER STAGE FORECASTS ARE BASED ON OBSERVED AND PREDICTED RAINFALL. IF
ACTUAL RAINFALL VARIES FROM FORECAST VALUES...FORECAST RIVER STAGES WILL VARY
ACCORDINGLY.</instruction>
```

The ECIG guidelines would concatenate the description and instruction field.

The WG is aware that these messages are only being sent to the test server, but it is unclear what, if any, changes will be made to the format and content of these messages before they go live. The NWS continues work on business rules, SAME message replication methods and programming code to create CAP EAS messages at a central facility for the IPAWS production platform.

6.4.2 Recommendations

1. We recommend that the NWS publish guidance that can be used for text to speech, to the extent that they do not (substantially) conflict with existing standards and practices already adopted within TTS engines.

2. We recommend that a set of acceptance criteria be developed, with the input of the broadcast/cable community, and that these criteria be met before NWS messages are made available on the production IPAWS OPEN system.

3. We recommend that the NWS and FEMA consider that the general CAP description and instruction fields do not allow the NWS to maintain its existing formats used by legacy data consumers while also being useful for direct to the public automated broadcast. Therefore an additional broadcast data field, such as the EASText field recommended by ECIG, but not accepted by FEMA, should be reconsidered.

This space left intentionally blank

7 Best Practices

7.1 Best Practice for Message Origination

As part of the Working Groups discussions, we observed the need for a set of best practices to guide both emergency managers and the systems development community in the process of CAP EAS message origination. While additional effort may be needed here to assist both emergency management and product developers, we assembled the following set of best practices as a starting point.

Before you begin, complete the following:

1. Complete the FEMA IPAWS Basic Course IS-247.a
2. Message origination tool must comply with CAP 1.2 protocol, IPAWS 1.0 profile and ECIG implementation guide.
3. Have proper credentials and digital signatures for the CAP aggregator for which you are originating.
4. Review your particular State's FCC approved State Plan.

CAUTION: CAP is a very useful tool to originate and disseminate emergency information over a variety of platforms. CAP is very versatile, but in order for CAP messages to be processed by the Emergency Alert System on radio, television, cable, and other EAS Participants, there are fields in a CAP message that are mandatory for EAS processing, even if they are optional for CAP.

7.2 CAP Message Preparation

One of the purposes of this document is to assist in preparation of CAP messages that will be ultimately broadcast on radio, television, cable and other media. The CAP origination tool that you have should assist you in this process. Most references in this document are to the ECIG Recommendation for CAP EAS Implementation Guide which may be found on the ECIG website.

Note: Before any CAP message is processed by an aggregator, it must conform to OASIS CAP v1.2. The message should also conform to the current FEMA CAP Profile, which may be found at www.fema.gov/.

7.3 EAS and CAP Audio

Audio can be a critical component of an EAS message. CAP provides at least two basic methods for audio to be transported and inserted in a resultant EAS message.

- An audio file can be inserted as a resource block, i.e. a uniform reference identifier (URI) location for an audio file, and more specifically a uniform resource locator (URL), or
- The audio can be converted with Text to Speech from the description and instruction elements of the info block, in accord with the ECIG CAP-EAS Implementation Guidelines as formally adopted by the Commission.

Although Text to Speech is an optional by current FCC Part 11 rules, the originator must realize that without one of these two methods, no audio will be present in the resultant EAS message. The only audible sound the listener will hear will be the EAS header codes, the Attention Signal, and the End-of-Message signal. Note that IPAWS currently depends on Text-to-Speech conversion.

> **Note**: IPAWS currently depends on Text-to-Speech conversion. CAP Message Checklist
>
> See EAS CAP Industry Group (ECIG) Recommendations for a CAP EAS Implementation Guide, Version 1.0. Section 6.7
> Web: http://eas-cap.org/ECIG-CAP-to-EAS_Implementation_Guide-V1-0.pdf

7.4 Best Practice for "Text to Speech"

A notification can be up to 1,800 characters and spaces in length, due to limitations on broadcast and cable video displays. Various CAP message origination tools may allow message originators to enter text that would be incorporated in the <description> and/or <instruction> elements of a CAP message. This text would be rendered into synthetic speech by enabled CAP EAS devices, when such a message is received (assuming a voice audio file was not present).

7.5 Message Originators

Message Originators should bear in mind that the content they input for text-to-speech would also be viewed on screen via TV and cable systems. For this reason, phonetic renderings of text should be avoided. To handle certain words, lexicons may need to be adjusted in CAP EAS device over time. In addition, message originators should avoid excessive use of acronyms or jargon.

7.6 Alert Messages

Alert messages should optimally be succinct and to-the-point. If an alert message contains many words and characters, originators should make use of punctuation such as periods and commas. This can better pace the synthetic speech rendering of the sentences and helps the message content flow evenly and properly. It can also prevent run-on sentences and incorrect intonation, which may confuse the recipient and prevent him/her from understanding the content of the message.

7.7 Entry of Address or Extensions

As a general convention, entry of addresses or extensions with a large number of digits may necessitate use of a space between each number.

For example, 32457 Safety Road should be entered in as 3 2 4 5 7 Safety Road.

7.8 Reference Guidelines

Refer to the stylistic guidelines indicated in FEMA's IS-247 training course
(Lesson 2: Appropriate, Effective, and Accessible Alert and Warning Messages), as well as the style guide recommendations listed in the EAS Style Guide Appendix.

7.9 Best Practice for SSL

CAP/EAS devices are, for the most part, unattended, embedded processor type systems. User maintenance interactions need to be limited. Some user installations are remote and do not have inbound Internet access for security reasons.

7.9.1 Common Root Certificates

CAP/EAS devices will have a set of common Root CA certificates that are updated slowly. They may not be up to date with intermediate certificates. To avoid the necessity of loading intermediate certificates, in the larger world of desktops, it has become a common practice for a web server to send the server certificate as well as the various chained intermediate certificates.

Similarly, in the specialized environment of CAP/EAS device, sending the chain will allow the CAP/EAS device to verify the chain of trust with only information from the SSL connection alone, as long the device has the applicable Root CA certificate.

If a CAP server wants to use HTTPS/SSL access and support the widest range of CAP/EAS devices, it must send all of the chained certificates (not including the Root CA) for SSL connections.

A CAP/EAS device must provide a means for its users to update the store of Root CA certificates, either by a firmware update, or a special certificate update.

CAP server owners should be aware that a change to the Root CA for its certificate chain, especially when a new CA is used, might cause CAP/EAS devices to not be able to connect to their server until the device manufactures can issue an update.

In addition, self-signed certificates may not work with all CAP/EAS devices, and should be avoided.

This space left intentionally blank

Appendix - EAS Style Guide

The EAS Style Guide is intended to assist CAP originators in formulating the optional fields of a CAP message that will be used for text-to-speech conversion, and display by character generators and various graphic platforms.

EAS Messages	All EAS messages are public; therefore, no information of a restricted or private nature should be included.
EAS Text	All EAS text should support, not contradict information that may be contained in an encapsulated audio message that is a part of the CAP message.
FCC Mandatory EAS Text	Information derived from the FCC Mandatory EAS text, (i.e., originator, event type, location, expiration) will already have been displayed, so it is not necessary to repeat all of the information contained in the FCC Mandatory EAS text EXCEPT for information of peculiar interest to the hearing impaired community.
EAS Phrasing	The EAS text must be fairly formal in its phrasing, but should not make over-use of highly technical or discipline specific jargon. EAS text should be for a target audience of third grade vocabulary and syntax.
Expression	Expression should be clear and concise.
Message Details	Details should be specific but must be limited to 1800 characters in order to fit within the constraints of a two-minute audio message. Important details should be repeated, but not lengthy.
Additional Message Details	EAS text may be used to amplify or provide additional details about an emergency situation but should not be overly repetitive.
Description of Emergency	The first thing to convey is a brief description of the emergency; the second thing to describe is the action that the listener/viewer needs to take immediately; the third thing to describe is a pointer for additional details.
EAS Language	The EAS is designed to “wake up” listeners/viewer to an emergency condition, not provide a journalistic detail of events.

Glossary

AFSK	Audio frequency-shift keying (AFSK) is a modulation technique by which digital data is represented by changes in the frequency (pitch) of an audio tone, yielding an encoded signal suitable for transmission via radio or telephone. Normally, the transmitted audio alternates between two tones: one, the "mark", represents a binary one; the other, the "space", represents a binary zero.
BRAPS	The somewhat annoying sound you hear just prior to an EAS Test or EAN.
CAP	Common Alerting Protocol, an XML-based data format for exchanging public warnings and emergencies between alerting technologies. CAP allows a warning message to be consistently disseminated simultaneously over many warning systems to many applications.
CSRIC	Communications, Security, Reliability, and Interoperability Council, FCC sponsored committees that provide analysis and recommendations.
EAN	An Emergency Action Notification (SAME code: EAN) is the national activation of the Emergency Alert System (EAS) and can only be activated by the President or their representative (i.e. the Vice President). The Emergency Broadcast System (EBS) also carried the Emergency Action Notification.
EAS	Emergency Alert System, The primary warning system that provides the President with the means to address the nation during a national crisis.
ECIG	The EAS-CAP Industry Group (ECIG) is a coalition of Emergency Alert System equipment, software and service providers.
FEMA	The Federal Emergency Management Agency (FEMA) is an agency of the United States Department of Homeland Security.
HTTP	The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.
IPAWS	Integrated Public Alert and Warning System, a planned multi-agency emergency population warning system in the United States. It is designed to provide rapid, reliable and effective communication to the public in case of major emergencies such as natural disasters and terrorist attacks.

IPAWS Open	FEMA is implementing the IPAWS Open Platform for Emergency Networks (IPAWS-OPEN) to collect CAP alerts issued by authorized public officials and distribute them to EAS Participants via an EAS CAP feed. The EAS CAP feed will be available via the Internet; therefore EAS Participants will require an Internet connection to poll IPAWS-OPEN. In addition, EAS Participants may poll state CAP servers or other CAP-based networks via the Internet where appropriate.
MP3	MPEG-1 or MPEG-2 Audio Layer III more commonly referred to as MP3, is a patented encoding format for digital audio which uses a form of lossy data compression. It is a common audio format for consumer audio storage, as well as a de facto standard of digital audio compression for the transfer and playback of music on most digital audio players.
NOAA	The National Oceanic and Atmospheric Administration (NOAA) (pronounced like "Noah") is a scientific agency within the United States Department of Commerce focused on the conditions of the oceans and the atmosphere. NOAA warns of dangerous weather, charts seas and skies, guides the use and protection of ocean and coastal resources, and conducts research to improve understanding and stewardship of the environment.
NWS	The National Weather Service (NWS), once known as the Weather Bureaus a part of National Oceanic and Atmospheric Administration (NOAA) of the United States government. It is headquartered in Silver Spring, Maryland.
OASIS	OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society
RDS	Radio Data System is a standard communications protocol (defined by the National Radio Systems Committee in the United States and adopted worldwide by International Electro-technical Commission) standard for embedding small amounts of digital information in conventional FM radio broadcasts.
SAME	Specific Area Message Encoding, The SAME header (help·info) is the most critical part of the EAS design. It contains information about who originated the alert (the President, state or local authorities, the National Weather Service (NOAA/NWS), or the broadcaster), a short, general description of the event (tornado, flood, severe thunderstorm), the areas affected (up to 31 counties or states), the expected duration of the event (in minutes), the date and time it was issued (in UTC), and an identification of the originating station. (See SAME for a complete breakdown of the header.)

SSL	Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet.TLS and SSL encrypt the segments of network connections at the Application Layer for the Transport Layer, using asymmetric cryptography for key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity.
XML	Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

Appendix References

- FCC EAS Rules (CFR 47 Part 11). Web:
  http://ecfr.gpoaccess.gov/cgi/t/text/textidx?c=ecfr&rgn=div5&view=text&node=47:1.0.1.1.11&idno=47
  http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr;sid=cc3136010c146f0321fadb5c8ecd228c;rgn=div5;view=text;node=47%3A1.0.1.1.12;idno=47;cc=ecfr

- FCC Second Report and Order, in the Matter of the Review of the Emergency Alert System, EB Docket No. 04-296, Adopted: May 31, 2007

- FCC Fourth Report and Order, in the Matter of the Review of the Emergency Alert System, EB Docket No. 04-296, Adopted: September 15, 2011

- FCC Fifth Report and Order, in the Matter of the Review of the Emergency Alert System, EB Docket No. 04-296, Adopted: January 9, 2012

- CAP v1.2 USA IPAWS Profile v1.0 Committee Specification OASIS Emergency Management Technical Committee, October 2009.
  Web: http://docs.oasis-open.org/emergency/cap/v1.2/ipaws-profile/v1.0/cap-v1.2-ipaws-profile-v1.0.pdf

- EAS CAP Industry Group (ECIG) Recommendations for a CAP EAS Implementation Guide, Version 1.0.
  Web: http://eas-cap.org/ECIG-CAP-to-EAS_Implementation_Guide-V1-0.pdf

- Receiver Performance Specification for Public Alert Receivers, CEA-2009-B (ANSI), November 01, 2010
  Web: http://www.ce.org/Standards/Standard-Listings/R3-Audio-Systems/CEA-2009-B-(ANSI).aspx

- National Weather Service Directive System 10-1712, NOAA Weather Radio (NWR) Specific Area Message Encoding (SAME), October 3, 2011
  Web: http://www.nws.noaa.gov/directives/sym/pd01017012curr.pdf

- CSRIC III WG #9 Final report part 1 submitted March 2012, part 2 submitted June 2012, and part 3 submitted September 2012.