Common Alerting Protocol, v. 1.1 USA Integrated Public Alert and Warning System Profile

Working Draft 05

12 February 2009

Specification URIs:
This Version:
http://docs.oasis-open.org/emergency/cap/v1.1/ipaws-profile/wd01/CAP-v1.1-IPAWS-Profile-WD01.html
http://docs.oasis-open.org/emergency/cap/v1.1/ipaws -profile/wd01/CAP-v1.1-IPAWS-Profile-WD01.doc
http://docs.oasis-open.org/emergency/cap/v1.1/ipaws -profile/wd01/CAP-v1.1-IPAWS-Profile-WD01.pdf

Previous Version:
http://docs.oasis-open.org/emergency/cap/v1.1/ipaws -profile/wd01/CAP-v1.1-IPAWS-Profile-WD01.html
http://docs.oasis-open.org/emergency/cap/v1.1/ipaws -profile/wd01/CAP-v1.1-IPAWS-Profile-WD01.doc
http://docs.oasis-open.org/emergency/cap/v1.1/ipaws -profile/wd01/CAP-v1.1-IPAWS-Profile-WD01.pdf

Latest Version:
http://docs.oasis-open.org/emergency/cap/v1.1/ipaws -profile/wd01/CAP-v1.1-IPAWS-Profile-WD01.html
http://docs.oasis-open.org/emergency/cap/v1.1/ipaws -profile/wd01/CAP-v1.1-IPAWS-Profile-WD01.doc
http://docs.oasis-open.org/emergency/cap/v1.1/ipaws -profile/wd01/CAP-v1.1-IPAWS-Profile-WD01.pdf

Technical Committee:
OASIS Emergency Management TC

Chair(s):
Sukumar Dwarkanath, SRA International
Tom Ferrentino, Individual
Elysa Jones, Warning Systems, Inc.

Editor(s):
Art Botterell, Contra Costa County Community Warning System
Rex Brooks, Individual
Sukumar Dwarkanath, SRA International

Related work:
This specification is related to:

- OASIS Standard CAP-V1.1, October 2005
- OASIS Standard CAP-V1.1, Approved Errata 2 October 2007

Declared XML Namespace(s):
urn:oasis:names:tc:emergency:cap:1.1

Abstract:

This profile of the XML-based Common Alerting Protocol (CAP) describes an interpretation of the OASIS CAP v1.1 standard necessary to meet the needs of the Integrated Public Alert and Warning System (IPAWS), a public alerting "system of systems" created by the U.S. Federal Emergency Management Agency.

Status:

This document was last revised or approved by the Emergency Management Technical Committee on the above date. The level of approval is also listed above. Check the current location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Emergency Management TC web page at **http://www.oasis-open.org/committees/emergency/.**

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page at **http://www.oasis-open.org/committees/emergency/ipr.php**

The non-normative errata page for this specification is located at **http://www.oasis-open.org/committees/emergency/.**

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as REQUIRED to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The names "OASIS", [insert specific trademarked names and abbreviations here] are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/who/trademark.php for above guidance.

Table of Contents

1 Introduction

1.1 Purpose

In order to meet the needs of the devices intended to receive alerts from the United States Integrated Public Alert and Warning System (IPAWS) System of Systems (SoS), this CAP v1.1 IPAWS Profile constrains the CAP v1.1 standard for receipt and translation with and among IPAWS exchange partners.

The use of this profile is not necessarily limited to the initial IPAWS Exchange Partners. It is available to all who might want to use the particular concepts defined in this specification.

The Common Alerting Protocol (CAP) provides an open, non-proprietary digital message format for all types of alerts and notifications. It does not address any particular application or telecommunications method. The CAP format is compatible with emerging techniques, such as Web services, as well as existing formats including the Specific Area Message Encoding (SAME) used for the United States' National Oceanic and Atmospheric Administration (NOAA) Weather Radio and the Emergency Alert System (EAS), while offering enhanced capabilities that include:

- Flexible geographic targeting using latitude/longitude shapes and other geospatial representations in three dimensions;
- Multilingual and multi-audience messaging;
- Enhanced message update and cancellation features;
- Template support for framing complete and effective warning messages;
- Compatible with digital encryption and signature capability; and,
- Facility for digital images and audio.

The Common Alerting Protocol (CAP) v1.0 and v1.1 were approved as OASIS standards before the Emergency Data Exchange Language (EDXL) project was developed. However, this profile specification shares the goal of the EDXL project to facilitate emergency information sharing and data exchange across the local, state, tribal, national and non-governmental organizations of different professions that provide emergency response and management services. Several exchange partner alerting systems of the IPAWS SoS are identified by this profile for specific accommodation. However, the CAP v1.1-IPAWS Profile is not limited to systems. It is structured to allow inclusion of other alerting systems as deemed appropriate or necessary.

In addition to the definition of the term Profile in Section 1.2 Terminology, this profile is responsive to the requirements articulated by the FEMA IPAWS Program Management Office as cited in Section 1.5 Non-Normative References..

1.2 Process

This Profile was developed primarily by integrating requirements related to three federal warning-delivery systems:

- the broadcast Emergency Alert System (EAS) as recommended by the EAS-CAP Industry Working Group;
- the NOAA Non-Weather Emergency Message (NWEM) "HazCollect" program for weather radio and other delivery systems as derived from technical documentation; and,
- the Commercial Mobile Alerting Service (CMAS) for cellular telephones as described in the recommendations of the Commercial Mobile Service Alert Advisory Committee (CMSAAC).

Additional guidance was drawn from subject matter experts familiar with the design and implementation of those and other public warning systems.

1.3 Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in **[RFC2119]**.

The words **warning, alert** and **notification** are used interchangeably throughout this document.

The term **coordinate pair** is used in this document to refer to a comma-delimited pair of decimal values describing a geospatial location in degrees, unprojected, in the form “[latitude],[longitude]”. Latitudes in the Southern Hemisphere and longitudes in the Western Hemisphere are signed negative by means of a leading dash.

CMAS – Commercial Mobile Alert System – System recommended by FCC-established Commercial Mobile Service Alert Advisory Committee (CMSAAC) CMSAAC's mission was to develop recommendations on technical standards and protocols to facilitate the ability of commercial mobile service (CMS) providers to voluntarily transmit emergency alerts to their subscribers. The committee was established pursuant to Section 603 of the Warning, Alert and Response Network Act (WARN Act), which was enacted on October 13, 2006.

DateTime Data Type - All CAP 1.1 dateTime elements (sent, effective, onset and expires) SHALL be specified in the form "YYYY-MM-DDThh:mm:ssXzh:zm" where:

- YYYY indicates the year
- MM indicates the month
- DD indicates the day
- T indicates the symbol “T” marking the start of the required time section
- hh indicates the hour
- mm indicates the minute
- ss indicates the second
- X indicates either the symbol “+” if the preceding date and time are in a time zone ahead of UTC, or the symbol “-‘ if the preceding date and time are in a time zone behind UTC. If the time is in UTC, the symbol “-“ will be used.
- zh indicates the hours of offset from the preceding date and time to UTC, or “00” if the preceding time is in UTC
- zm indicates the minutes of offset from the preceding date and time to UTC, or “00” if the preceding time is in UTC

For example, a value of “2002-05-30T09:30:10-05:00” would indicate May 30, 2002 at 9:30:10 AM Eastern Standard Time, which would be 2:30:10PM Universal Coordinated Time (UTC). That same time might be indicated by “2002-05-30T14:30:10-00:00”.

DHS – USA Department of Homeland Security – Federal Executive Branch Cabinet Department

EAS – USA Emergency Alert System, specifically mandated by the FCC is a national public warning system that requires broadcasters, cable television systems, wireless cable systems, satellite digital audio radio service (SDARS) providers and, direct broadcast satellite (DBS) service providers to provide the communications capability to the President to address the American public during a National emergency. The system also may be used by state and local authorities to deliver important emergency information such as AMBER alerts and weather information targeted to a specific area.

FCC – USA Federal Communication Commission.

FEMA – USA Federal Emergency Management Agency

HazCollect – USA National Oceanic and Atmospheric Administration, National Weather Service All Hazards Emergency Message Collection System (HazCollect) provides an automated capability to streamline the creation, authentication, collection, and dissemination of non-weather emergency messages in a quick and secure fashion. The HazCollect system is a comprehensive solution for the centralized collection and efficient distribution of Non-Weather Emergency Messages (NWEMs) to the NWS dissemination infrastructure, the Emergency Alert System (EAS), and other national systems.

IPAWS – USA Integrated Public Alert and Warning System was established by Executive Order 13407 in June 2006. The Department of Homeland Security, the Federal Emergency Management Agency (DHS/FEMA) and the IPAWS Program Management Office (PMO) work with public and private sectors to integrate warning systems to allow the President and authorized officials to effectively address and warn the public and State and local emergency operations centers via phone, cell phone, pagers, computers and other personal communications devices

IPAWS Exchange Partner –The EAS, HazCollect and CMAS exchange partners are specifically addressed by this specification document. Other systems may also use this profile.

Profile – As used in this document, a profile consists of an agreed-upon subset and interpretation of the. OASIS CAP-v1.1 Specification.: An XML Profile is applied to an existing XML Schema (in this case the OASIS Standard CAP v1.1 Schema) in order to constrain or enforce aspects of it to accomplish a specific purpose according to the definition and criteria set forth for an XML Profile. Any message that is in compliance with the Profile must validate against the original XML Schema as well as the resulting XML Schema of the Profile.

1.4 Normative References

[RFC2119]	S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, IETF RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt
[dateTime]	N. Freed, XML Schema Part 2: Datatypes Second Edition, http://www.w3.org/TR/xmlschema-2/#dateTime , W3C REC-xmlschema-2, October 2004.
[FIPS 180-2]	National Institute for Standards and Technology, Secure Hash Standard, August 2002. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf
[namespaces]	T. Bray, Namespaces in XML, W3C REC-xml-names-19990114, January 1999. http://www.w3.org/TR/REC-xml-names/
[**RFC2046]**	N. Freed, Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types, IETF RFC 2046, November 1996. http://www.ietf.org/rfc/rfc2046.txt

[RFC2119] S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, IETF RFC 2119, March 1997.
http://www.ietf.org/rfc/rfc2119.txt

[RFC3066] H. Alvestrand, Tags for the Identification of Languages, IETF RFC 3066, January 2001.
http://www.ietf.org/rfc/rfc3066.txt

[WGS 84] National Geospatial Intelligence Agency, Department of Defense World Geodetic System 1984, NGA Technical Report TR8350.2, January 2000.
`
http://earth-info.nga.mil/GandG/tr8350_2.html

[XML 1.0] T. Bray, Extensible Markup Language (XML) 1.0 (Third Edition), W3C REC-XML-20040204, February 2004.
http://www.w3.org/TR/REC-xml/

[XMLSIG] Eastlake, D., Reagle, J. and Solo, D. (editors), *XML-Signature Syntax and Processing*, W3C Recommendation, February 2002.
http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

[XMLENC] Eastlake, D. and Reagle, J. (editors), *XML Encryption Syntax and Processing*, W3C Recommendation, December 2002.
http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

[CFR Title 47 Pt 11] Office of the Federal Register, National Archives and Records Administration, Government Printing Office, *XML Code of Federal Regulations, Federal Communications Commission*, Title 47 Telecommunication Part 11 Emergency Alert System, October 1998.
http://www.access.gpo.gov/nara/cfr/waisidx_98/47cfr11_98.html

1.5 Non-Normative References

[FEMA IPAWS CAP PROFILE REQUIREMENTS]	FEMA IPAWS Program Management Office *FEMA IPAWS CAP v1.1 Profile Requirements v2.4 - Public*, December 2008 http://www.oasis-open.org/committees/download.php/31084/FEMA_IPAWS_CAP%20v1.1_Profile_Requirements_v2.4_-_Public.doc
[EAS-CAP PROFILE]	EAS-CAP Industry Group *EAS-CAP Profile Recommendation EAS-CAP-01*, September 2008. http://www.eas-cap.org/Recommendation%20EAS-CAP-0.1.pdf
[**NOAA HazCollect]**	Disaster Management Open Platform for Emergency Networks Program *Instructions for Using the NOAA HazCollect Interface on the Open Platform for Emergency Networks (OPEN)* November 2008
.	http://www.oasis-open.org/committees/download.php/31085/using_hazcollect_on_open20081106.pdf

2 CAP v1.1 IPAWS Profile

The follow table specifies the REQUIRED constraints placed by the CAP v1.1 IPAWS Profile on a CAP v1.1 message in order for the message to be a valid CAP IPAWS Profile message. This table contains only those elements of CAP v1.1 for which there is a Profile Specification or Profile Note. CAP v1.1 elements not included here simply means there is no specific constraint or condition in the use of those elements for the Profile.

Table 1: CAP v1.1 IPAWS Profile Specification and Profile Note

CAP Element	Profile Specification (Normative)	Profile Note (Non-Normative)
	(Subcommittee)	(Subcommittee)
sent	(1) The XML dateTime value SHALL include the timezone offset.	
status	(1) A value of "Actual" SHALL be used for messages intended for dissemination to the public, including test messages intended for delivery to the public.	es of status “Actual” based on those y EAS required weekly test messages.
source		(1) Implementers should be aware that the <source> value may be publicly presented as a "signature" line in some delivery systems.
code *	(1) REQUIRED. Value SHALL include the string "IPAWSv1.0" to indicate the profile version in use.	
references	(1) All messages that have not yet expired should be referenced for messages of type “update” or “cancel”.	
info *	(2) All info blocks in a single alert MUST relate to a single incident or update, with the same category and eventCode values. (3) All info blocks SHALL be appropriate for immediate public release.	(1) Multiple info blocks may be used for the same message in different languages. (2) If additional info blocks are present, IPAWS System Partners MAY process only the first info block.

CAP Element	Profile Specification (Normative)	Profile Note (Non-Normative)
responseType *		(1) Use of the non-standard value "Avoid" is a recognized exception to the CAP 1.1 specification. (2) Use of this value will not validate against the CAP v1.1 schema.
eventCode *	(1) Messages intended for EAS, CMAS and HazCollect dissemination MUST include an instance of this with a valueName of "SAME" and using a SAME-standard three-letter value. (2) Other eventCode elements may also be present. (3) All values for EAS Event Code SHALL be passed through by EAS CAP Profile devices, even if the Event Code is not shown in FCC Part 11.31, as long as the value is a three-letter code and is approved by the FCC.	
effective	(1) Ignored if present. Alerts SHALL be effective upon issuance. (2) However, the description and/or instruction may refer to future events or actions.	
onset	(1) Ignored if present. Alerts SHALL be effective upon issuance. (2) However, the description and/or instruction may refer to future events or actions.	
expires	(1) REQUIRED. The XML dateTime value MUST include the timezone offset.	

CAP Element	Profile Specification (Normative)	Profile Note (Non-Normative)
parameter *	(1) Message intended for EAS and/or HazCollect dissemination MUST include a parameter with a valueName of "EAS-ORG" with a value of SAME ORG code. (2) Messages invoking the "Gubernatorial Must-Carry" rule SHALL also include a parameter with valueName of "EAS-Must-Carry" and value of "TRUE" for gubernatorial alerts. (3) OPTIONAL free-form text for CMAS MAY be included in a parameter with valueName of "CMAMtext". (4) There is a 90 English character limit in the free form text. (5) Other parameter elements may also be present.	The handling of free form CMAS text messages is still TBD.
resourceDesc	(1) A value of "EAS Broadcast Content" SHALL be used to indicate that the audio, video or image content of the current <resource> is intended for EAS broadcast.	
mimeType	(1) Recorded audio for delivery to the public SHALL be identified and encoded in one of the following formats: a. As “audio/x-ipaws-audio-mpeg”, encoded as MPEG Layer 3 (MP3) audio, 64kbps, 22.05 or 44.1 kHz sampling; or, b. As “audio/x-ipaws-audio-wav”, encoded as WAV PCM, mono, 16-bit, 22.05 kHz sampling. (2) Streaming audio for delivery to the public SHALL be identified as “audio/x-ipaws-streaming-audio-mpeg” and SHALL be MP3 audio, 64kbps, 22.05 or 44.1 kHz sampling, and transported via HTTP or Shoutcast/Icecast service. (3) Additional MIME types and encodings for other media formats such as video may be specified by the United States Department of Homeland Security using the “x-ipaws-“ prefix in the parameter portion of the	

	MIME designator type.	
CAP Element	**Profile Specification (Normative)**	**Profile Note (Non-Normative)**
area *	(1) At least one <area> element MUST be present. (2) All <area> elements SHALL be considered in message distribution.	
geocode *	(1) At least one instance REQUIRED with a valueName of "SAME" and value of a SAME 6-digit location code (extended FIPS). (2) A SAME value of “000000” refers to ALL United States territoriy.	(1) The 5-digit form, if needed, can be derived by removing the first digit from the 6 digit form.

*May have multiple occurrences in a message under CAP 1.1 spec

3 Conformance

An implementation conforms to this specification if it satisfies all of the MUST or REQUIRED level requirements defined within this specification.

This specification references a number of other specifications. In order to comply with this specification, an implementation MUST implement the portions of referenced specifications necessary to comply with the required provisions of this specification. Additionally, the implementation of the portions of the referenced specifications that are specifically cited in this specification MUST comply with the rules for those portions as established in the referenced specification.

3.1 Conformance Targets

The two following conformance targets are defined in order to support the specification of conformance to this standard:

a) CAP V1.1 IPAWS PROFILE Message
b) CAP V1.1 IPAWS PROFILE Message Producer
c) CAP V1.1 IPAWS PROFILE Message Consumer

A CAP V1.1 IPAWS PROFILE Message is an XML 1.0 document whose syntax and semantics are specified in this standard.

A CAP V1.1 IPAWS PROFILE Message Producer is a software entity that produces CAP V1.1 IPAWS PROFILE Messages.

3.2 Conformance as an CAP V1.1 IPAWS Profile Message

An XML 1.0 document is a conforming CAP V1.1 IPAWS PROFILE Message if and only if:

a) it is valid according to the schema located at http://docs.oasis-open.org/emergency/CAPv1.1-IPAWS-Profile-v1.0 .xsd ; (placeholder) and
b) the content of its elements and the values of its attributes meet all the additional mandatory requirements specified in Section 2.

3.3 Conformance as an CAP V1.1 IPAWS Profile Message Producer

A software entity is a conforming CAP V1.1 IPAWS PROFILE Message Producer if and only if:

it is constructed in such a way that any XML document produced by it and present in a place in which a conforming CAP V1.1 IPAWS PROFILE Message is expected (based on contextual information) is indeed a conforming CAP V1.1 IPAWS PROFILE Message according to this standard.

The condition in (1) above can be satisfied in many different ways. Here are some examples of possible scenarios:

– a standard protocol (for example, EDXL-DE) transfers messages carrying CAP V1.1 IPAWS PROFILE Messages; a client has sent a request for an CAP V1.1 IPAWS PROFILE Message to a server which claims to be a conforming CAP V1.1 IPAWS PROFILE Message Producer, and has received a response which is therefore expected to carry a conforming CAP V1.1 IPAWS PROFILE Message;
– a local test environment has been set up, and the application under test (which claims to be a conforming CAP V1.1 IPAWS PROFILE Message Producer) has the ability to produce a CAP V1.1 IPAWS PROFILE Message and write it to a file in a directory in response to a request coming from the testing tool; the testing tool has sent many requests to the application under test and is now verifying all

the files present in the directory, which is expected to contain only conforming CAP V1.1 IPAWS PROFILE Messages;

3.4 Conformance as an CAP V1.1 IPAWS Profile Message Consumer

A software entity is a conforming CAP V1.1 IPAWS PROFILE Message Consumer if and only if:

it is constructed in such a way that it is able to successfully validate and ingest a CAP V1.1 IPAWS PROFILE Message, as defined in Sec 1.2

The condition in (1) above can be satisfied in many different ways. Here is one example of a possible scenario:

– a client receives and processes a CAP V1.1 IPAWS PROFILE Message from a server which claims to be a conforming CAP V1.1 IPAWS PROFILE Message Producer

A. XML Schema for the CAPv1.1 IPAWS Profile (NORMATIVE)

```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:cap="urn:oasis:names:tc:emergency:cap:1.1" xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="urn:oasis:names:tc:emergency:cap:1.1" elementFormDefault="qualified"
attributeFormDefault="unqualified">
  <element name="alert">
    <annotation>
      <documentation>CAP 1.1 - IPAWS Profile 1.0 Alert Message</documentation>
    </annotation>
    <complexType>
      <sequence>
        <element name="identifier" type="string"/>
        <element name="sender" type="string"/>
        <element name="sent" type="dateTime">
<!-- Restriction using a regular expression or just annotate ?? -->
          <annotation>
            <documentation>dateTime value including timezone offset</documentation>
          </annotation>
        </element>
        <element name="status">
          <simpleType>
            <restriction base="string">
              <enumeration value="Actual"/>
              <enumeration value="Exercise"/>
              <enumeration value="System"/>
              <enumeration value="Test"/>
              <enumeration value="Draft"/>
            </restriction>
          </simpleType>
        </element>
        <element name="msgType">
          <simpleType>
            <restriction base="string">
              <enumeration value="Alert"/>
              <enumeration value="Update"/>
              <enumeration value="Cancel"/>
              <enumeration value="Ack"/>
              <enumeration value="Error"/>
            </restriction>
          </simpleType>
        </element>
        <element name="scope">
          <simpleType>
            <restriction base="string">
              <enumeration value="Public"/>
              <enumeration value="Restricted"/>
              <enumeration value="Private"/>
            </restriction>
          </simpleType>
        </element>
        <element name="restriction" type="string" minOccurs="0"/>
        <element name="addresses" type="string" minOccurs="0"/>
        <element name="code">
          <simpleType>
            <restriction base="string">
              <enumeration value="IPAWSv1.0"/>
            </restriction>
          </simpleType>
        </element>
        <element name="code" type="string" maxOccurs="unbounded"/>
        <element name="note" type="string" minOccurs="0"/>
        <element name="references" type="string" minOccurs="0"/>
        <element name="incidents" type="string" minOccurs="0"/>
```

```
      <element name="info" minOccurs="0" maxOccurs="unbounded">
       <complexType>
        <sequence>
         <element name="language" type="language" default="en-US" minOccurs="0"/>
         <element name="category" maxOccurs="unbounded">
          <simpleType>
           <restriction base="string">
            <enumeration value="Geo"/>
            <enumeration value="Met"/>
            <enumeration value="Safety"/>
            <enumeration value="Security"/>
            <enumeration value="Rescue"/>
            <enumeration value="Fire"/>
            <enumeration value="Health"/>
            <enumeration value="Env"/>
            <enumeration value="Transport"/>
            <enumeration value="Infra"/>
            <enumeration value="CBRNE"/>
            <enumeration value="Other"/>
           </restriction>
          </simpleType>
         </element>
         <element name="event" type="string"/>
         <element name="responseType" minOccurs="0" maxOccurs="unbounded">
          <simpleType>
           <restriction base="string">
            <enumeration value="Shelter"/>
            <enumeration value="Evacuate"/>
            <enumeration value="Prepare"/>
            <enumeration value="Execute"/>
            <enumeration value="Monitor"/>
            <enumeration value="Assess"/>
            <enumeration value="None"/>
           </restriction>
          </simpleType>
         </element>
         <element name="urgency">
          <simpleType>
           <restriction base="string">
            <enumeration value="Immediate"/>
            <enumeration value="Expected"/>
            <enumeration value="Future"/>
            <enumeration value="Past"/>
            <enumeration value="Unknown"/>
           </restriction>
          </simpleType>
         </element>
         <element name="severity">
          <simpleType>
           <restriction base="string">
            <enumeration value="Extreme"/>
            <enumeration value="Severe"/>
            <enumeration value="Moderate"/>
            <enumeration value="Minor"/>
            <enumeration value="Unknown"/>
           </restriction>
          </simpleType>
         </element>
         <element name="certainty">
          <simpleType>
           <restriction base="string">
            <enumeration value="Observed"/>
            <enumeration value="Likely"/>
            <enumeration value="Possible"/>
            <enumeration value="Unlikely"/>
            <enumeration value="Unknown"/>
           </restriction>
          </simpleType>
         </element>
         <element name="audience" type="string" minOccurs="0"/>
         <element name="eventCode">
```

```
            <complexType>
              <sequence>
                <element name="valueName">
                  <simpleType>
                    <restriction base="string">
                      <enumeration value="SAME"/>
                    </restriction>
                  </simpleType>
                </element>
                <element name="value">
                  <simpleType>
                    <restriction base="string">
                      <minLength value="3"/>
                      <maxLength value="3"/>
                    </restriction>
                  </simpleType>
                </element>
              </sequence>
            </complexType>
          </element>
          <element name="eventCode" minOccurs="0" maxOccurs="unbounded">
            <complexType>
              <sequence>
                <element ref="cap:valueName"/>
                <element ref="cap:value"/>
              </sequence>
            </complexType>
          </element>
          <element name="effective" type="dateTime" form="qualified" minOccurs="0"/>
          <element name="onset" type="dateTime" minOccurs="0"/>
          <element name="expires" type="dateTime" minOccurs="1" maxOccurs="1">
<!-- Restriction using a regular expression or just annotate ?? -->
            <annotation>
              <documentation>dateTime value including timezone offset</documentation>
            </annotation>
          </element>
          <element name="senderName" type="string" minOccurs="0"/>
          <element name="headline" type="string" minOccurs="0"/>
          <element name="description" type="string" minOccurs="0"/>
          <element name="instruction" type="string" minOccurs="0"/>
          <element name="web" type="anyURI" minOccurs="0"/>
          <element name="contact" type="string" minOccurs="0"/>
          <element name="parameter" maxOccurs="unbounded">
            <complexType>
              <sequence>
                <element ref="cap:valueName"/>
                <element ref="cap:value"/>
              </sequence>
            </complexType>
          </element>
          <element name="resource" minOccurs="0" maxOccurs="unbounded">
            <complexType>
              <sequence>
                <element name="resourceDesc" type="string"/>
                <element name="mimeType" type="string" minOccurs="0"/>
                <element name="size" type="integer" minOccurs="0"/>
                <element name="uri" type="anyURI" minOccurs="0"/>
                <element name="derefUri" type="string" minOccurs="0"/>
                <element name="digest" type="string" minOccurs="0"/>
              </sequence>
            </complexType>
          </element>
          <element name="area" minOccurs="1" maxOccurs="unbounded">
            <complexType>
              <sequence>
                <element name="areaDesc" type="string"/>
                <element name="polygon" type="string" minOccurs="0" maxOccurs="unbounded"/>
                <element name="circle" type="string" minOccurs="0" maxOccurs="unbounded"/>
                <element name="geocode">
                  <complexType>
                    <sequence>
```

```
                    <element name="valueName">
                      <simpleType>
                        <restriction base="string">
                          <enumeration value="SAME"/>
                        </restriction>
                      </simpleType>
                    </element>
                    <element name="value">
                      <simpleType>
                        <restriction base="integer">
                          <minLength value="6"/>
                          <maxLength value="6"/>
                        </restriction>
                      </simpleType>
<!--  Or this type of restriction using regular express instead
                      <simpleType>
                        <restriction base="integer">
                          <pattern value="[0-9][0-9][0-9][0-9][0-9][0-9]"/>
                        </restriction>
                      </simpleType>
-->
                    </element>
                  </sequence>
                </complexType>
              </element>
              <element name="geocode" minOccurs="0" maxOccurs="unbounded">
                <complexType>
                  <sequence>
                    <element ref="cap:valueName"/>
                    <element ref="cap:value"/>
                  </sequence>
                </complexType>
              </element>
              <element name="altitude" type="string" minOccurs="0"/>
              <element name="ceiling" type="string" minOccurs="0"/>
            </sequence>
          </complexType>
        </element>
      </sequence>
    </complexType>
  </element>
  <element name="valueName" type="string"/>
  <element name="value" type="string"/>
</schema>
```

B. FEMA IPAWS CAP v1.1 Profile Requirements v2.4 Public

The following document is included as an information resource for reference to the main set of requirements used as a basis for this specification. Where Appendix C compares the processing rules of the various IPAWS Exchange Partner Alerting Systems, this document concerns the overall IPAWS System and addresses design considerations that span the specific requirements of individual partner systems. Of particular interest is *Table 1 CAP v1.1 Profile Criteria and Miscellaneous Requirements* which specify high level design requirements for the purpose of satisfying IPAWS System-wide needs, with the caveat that EAS system requirements were of the most immediate concern. It should be noted that this profile specification is an OASIS work product and this reference document is offered to give the reader the context from which the OASIS Emergency Management Technical Committee conducted its work and this reference is not normative.

Federal Emergency Management Agency (FEMA)
Integrated Public Alert & Warning System (IPAWS)
Common Alerting Protocol (CAP) v1.1 Profile Requirements
Draft Version 2.4
December 10, 2008

Revision / Meeting History

Name	Date	Reason For Changes	Version
FEMA, OIC, JHU / APL	11/14/08	Meeting held to discuss recommendation and approach to move forward. Following this meeting the directed approach was pursued	1.0
DHS S&T	11/18/08	Initial Draft Document Conceptual design	1.0
DHS S&T	11/19/08	Fleshed out general approach to entire document with two major sections: 1- CAP v1.1– EAS specific portions of the IPAWS Profile and 2- Technical translation from this CAP v1.1-EAS portion of the IPAWS Profile to the FCC CFR Title 47 Part 11 target message structure.	1.1
DHS S&T	11/21/08	Draft CAP – EAS portion of the IPAWS Profile section and partial translation section	1.3
DHS S&T	11/23/08	Draft translation section with iterative revisions to the Profile section; Draft introductory sections	1.4
DHS S&T	11/24/08	First cut completion of all sections for final document flow and editing	1.5
DHS S&T	11/25/08	Final vetting, document flow and revision for review by OIC, JHU & FEMA	1.6
DHS S&T	11/26/08	Post internal review edits	1.7
FEMA	12/03/08	Embedded document comments received by FEMA with accompanying email	1.7
DHS S&T	12/05/08	Final revisions in response to FEMA comments	2.1
FEMA	12/09/08	Final revisions	2.2 and 2.3
FEMA	12/10/08	Editorial modifications	2.4

Table of Contents

Table of Figures and Tables

B.1 Introduction

The Federal Emergency Management Agency (FEMA) Integrated Public Alert and Warning System (IPAWS) provides the Nation's next generation public communications and warning capability. IPAWS enables the timely dissemination of alert and warnings before, during and after an emergency. FEMA and the IPAWS Program Management Office (PMO) work with the public and private sector to integrate warning systems that allow the President and authorized officials to effectively provide alerts to state and local Emergency Operations Centers (EOC) and the public via analog and digital television, radio, digital cable television, Digital Audio Broadcast (DAB), telephone, cell phone, pagers, computers, Direct Broadcast Satellite (DBS), Satellite Digital Audio Radio System (SDARS), and other communications methods. The Organization for the Advancement of Structured Information Standards (OASIS) Emergency Data Exchange Language Common Alerting Protocol (EDXL-CAP v1.1) will be used by IPAWS to facilitate the rapid delivery of alert and warnings across these various systems within the IPAWS System of Systems (SoS). CAP is the medium to enable an emergency manager to issue a single message that is disseminated through several different and distinct means to populations at risk. Throughout this document, the EDXL-CAP v1.1 will be referred to as CAP v1.1, and the words “warning,” “alert,” and “message” will be used interchangeably.

OASIS is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society. CAP v1.1 is a widely-used, fully-implemented, and mature data standard with a focus on alert and warning messages. By focusing on existing international standards, IPAWS and its exchange partners drastically reduce time require to develop and implement a message standard. Exchange partners are those communities of interest who agree to receive and disseminate IPAWS CAP v1.1-based alerts via their systems and networks.

This document draws from the research and analysis of four IPAWS message exchange partner documents, including draft deliverables and recommendations prepared to date. The following artifacts were analyzed:

- Industry Canada, Common Alerting Protocol Canadian Profile (CAPCP), v1.1, May 8, 2008, http://www.ic.gc.ca/epic/site/et-tdu.nsf/vwapj/CAPCPv1.1_May_8_2008_E.pdf/$FILE/CAPCPv1.1_May_8_2008_E.pdf
- Joint Alliance for Telecommunications Industry Solutions (ATIS)/ Telecommunications Industry Association (TIA), Commercial Mobile Alerting System (CMAS) Federal Alert Gateway to Commercial Mobile Service Provider (CMSP) Gateway Interface Specification, v0.18, September 19, 2008
- FEMA Disaster Management Open Platform for Emergency Networks (DM-OPEN), Instructions for Using the NOAA HazCollect Interface on the Open Platform for Emergency Networks (OPEN), v0.3, November 6, 2008, http://www.disasterhelp.gov/disastermanagement/library/documents/using_hazcollect_on_open20081106.pdf
- EAS-CAP Industry Group, EAS-CAP Profile Recommendation EAS-CAP-0.1, September 25, 2008 (referred to as the “ECIG Recommendation”), http://www.eas-cap.org/profile.htm

In order to meet the needs of the devices intended to receive alerts from IPAWS, an IPAWS CAP v1.1 Profile must be developed to constrain the CAP v1.1 standard for receipt and translation for each IPAWS exchange partner. A single CAP <alert> will be created at message origination with multiple <info> blocks – one <info>

block for each disparate exchange partner, as necessary. Several exchange partners will be added to the IPAWS SoS over time, beginning with the Emergency Alert System (EAS). At this time, the IPAWS CAP v1.1 Profile shall only address the adaptation of CAP for EAS. The Federal Communications Commission (FCC) Code of Federal Regulations (CFR) Title 47 Part 11 describes the EAS alert structure. However, future revisions of the CAP Profile provide specifications for future exchange partners as seen in Figure 1.

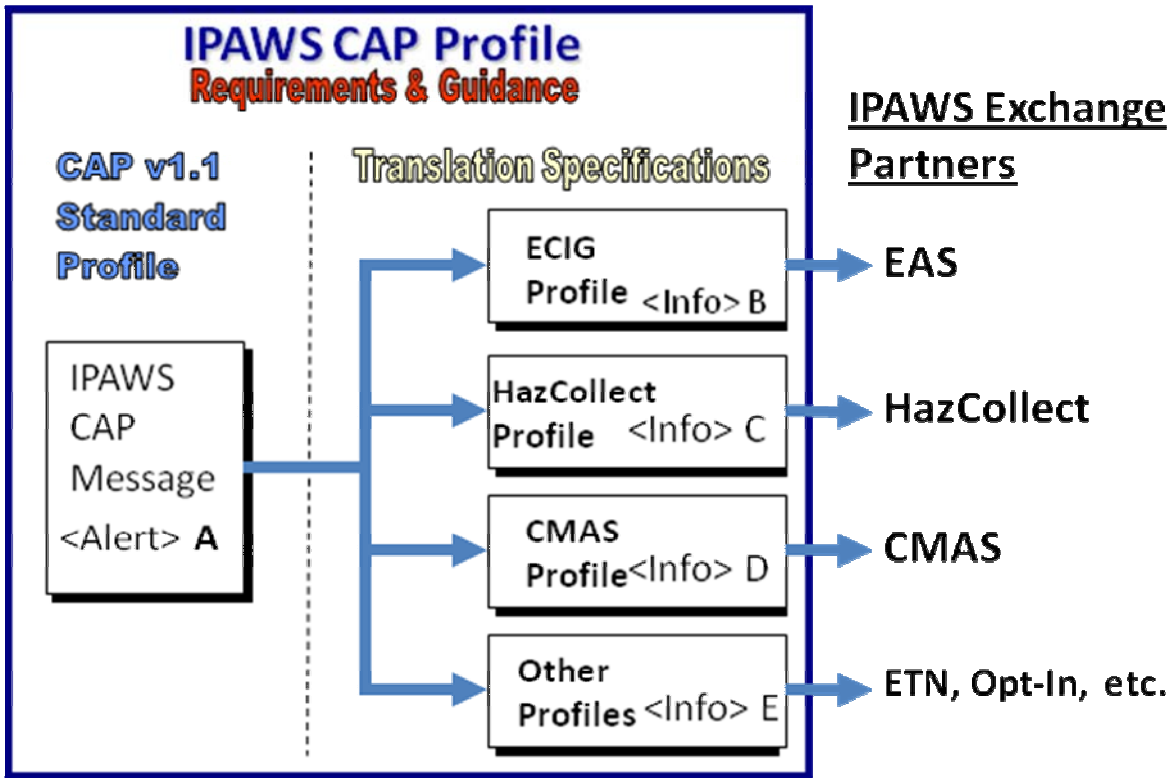


Figure 1- IPAWS-CAP v1.1 Profile Message Exchange Concept

B.1.1 Purpose

Because public warnings intended for transmission over the EAS can be encoded various ways in CAP, a standardized guideline is desired across all EAS equipment manufacturers and warning practitioners. The Department of Homeland Security (DHS) Office for Interoperability and Compatibility (OIC), FEMA and its practitioner representatives have prepared this document independently of vendor efforts with two purposes in mind:

1. To request that OASIS vet the requirements and recommendations for standardization of an OASIS CAP v1.1-EAS Profile. This Profile defines the source of any CAP v1.1-based alert message intended for transmission over the EAS
2. To provide a technical specification for equipment manufacturers for “translation” FROM this standardized OASIS CAP v1.1-EAS Profile TO the FCC CFR Title 47 Part 11 target message formats

B.1.2 Scope

IPAWS will initially design the capability to pass CAP v1.1 alerts and warnings to EAS, and addition systems such as the National Oceanic and Atmospheric Administration (NOAA) HazCollect and the Commercial Mobile Alert System (CMAS) will be added in the future. The primary usecase supported by IPAWS requires an

originator to create and send a message that complies with the IPAWS CAP v1.1 Profile structure. That message is automatically disseminated to multiple target systems or exchange partners. FEMA envisions the resulting CAP v1.1 structure as a single CAP v1.1 <alert> block that contains multiple <info> blocks – one per exchange partner as seen in Figure 2. The intent of IPAWS is to tailor one <info> block specifically for each particular exchange partner as necessary within criteria required for a profile.

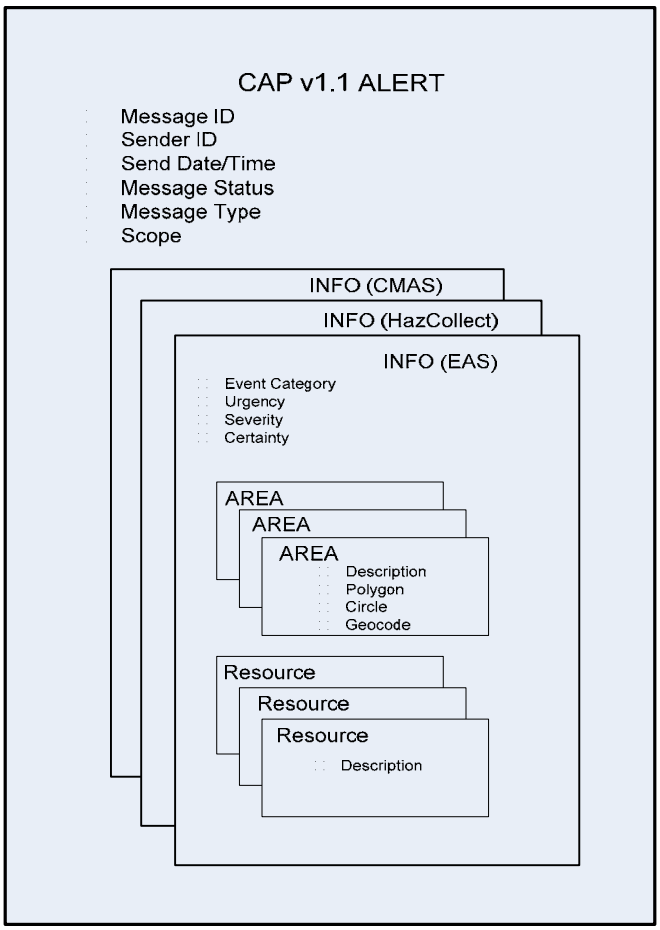


Figure 2- Single CAP v1.1 <alert>, containing multiple <info> blocks (one per Exchange Partner)

Options to encapsulate the IPAWS CAP v1.1 Profile by the EDXL-Distribution Element (DE) are possible and should be considered once enhanced routing and security methods are addressed; however, in this representation, application of EDXL-DE in this structure would be redundant with CAP v1.1 basic <alert> capabilities. CAP v1.1 was developed prior to the EDXL-DE, and therefore had routing capabilities built in. Under this structure, the <info> blocks are partner-specific requiring routing via the <alert> block. Therefore, this document (as did the ECIG recommendation) utilizes only CAP v1.1 as currently designed to perform routing and alerting (i.e., using the <alert> as the "header" for multiple <info> blocks). This document focuses on the construction of an <info> block tailored for EAS purposes and establishes a framework to add <info> blocks for other IPAWS exchange partners.

B.1.3 Approach

Although the ECIG recommendation was previously reviewed, this document was treated as an independent analysis through detailed research of the FCC 47 CFR Part 11 documentation. Upon completion, the results contained in this document were compared with the results of the ECIG recommendation. Though the ECIG recommendation is an extremely thorough and valuable body of work, some differences are presented for consideration.

This document is organized into two primary sections:

1. Profile Requirements: Presented in the form of requirements and guidelines that constrain CAP v1.1 for the construction of an EAS alert message. It is important to note that the CAP v1.1 Profile is not intended to become new messaging standards, but it is a only a constrained version of the existing CAP v1.1 standard
2. Technical Specifications: Presented in the form of detailed flowcharts and narrative. The flowcharts start with the IPAWS CAP v1.1 Profile message, step through the translation process, and result in an EAS alert. The process of technical specification development also helped to validate the definition of the IPAWS CAP v1.1-EAS Profile

The target message structure requires that the <alert> elements be harmonized over time and across exchange partners with conflicts resolved. <info> elements may be tailored by partner, but <alert> elements are common across partners. The methodology applied while proceeding through the CAP v1.1 elements list gives preference to EAS for each element interrogated. At this time, an element may be used for an EAS-specific application. As future exchange partners are added and conflicts arise, IPAWS CAP v1.1 extensions may then be added utilizing the <parameter> element. Adding information in <parameter> elements could duplicate the intent of some of the <alert> elements. However, every effort will be made to harmonize the existing elements prior to adding message exchange partner specific parameters.

B.2 IPAWS Description

IPAWS has been established to meet the Executive Order 13407, which requires "an effective, reliable, integrated, flexible, and comprehensive system to alert and warn the American people in situations of war, terrorist attack, natural disaster or other hazards to public safety and well being." The primary mission of IPAWS[1] is to assist the President address the nation of the critical alerts and warnings. The goal of IPAWS it to send all-hazards alerts and warnings to the greatest number of people, including those with disabilities and for who English is not his or her primary language. IPAWS shall be required to disseminate those messages over as many platforms as possible to ensure the widest dissemination.

B.2.1 IPAWS Scope

The scope of IPAWS has two dimensions. The first dimension is to become the end-to-end system of message dissemination. IPAWS provides the President with the capacity for immediate communication to the general public at the national, State and local levels during periods of national emergency. Governors, Mayors, public, and private sector entities may also use selected capabilities of IPAWS on a case-by-case basis as a means of emergency communication with the public in their State or localities.

The second dimension to the IPAWS is as an alert and warning medium. The three basic components of any communication are the message, the medium, and the audience, and IPAWS is the medium. It neither influences the message nor the audience; although, all three components interrelate. It provides a capacity to

[1] IPAWS Mission Needs Statement

transmit simultaneous translations of messages into one or more languages for all users, and it is the means available for disseminating alerts and warnings at all the levels of an incident. Within the domain of a message, there is an echelon of parties (i.e., national, State, local). There is an individual who sends the message (i.e., President of the United States, Governor, or Mayor). There is an organization that may be involved in this message (i.e., DHS, FEMA, NOAA, or CDC), and there are representatives at each of the separate echelons. The audience for that message is made up of organizations (Federal agencies, State governments, local governments, and the private sector) and individuals (people).

IPAWS is the means and the mechanism for that message to reach this audience. The mode can be broadcast (television, radio, internet) or targeted (telephone contact or Internet), but the means does not influence who provides the message, what the message says, or the intended audience. It is solely the manner through which the message is conveyed. IPAWS provides communications and interoperability capabilities that transcend Preparedness, Response and Recovery – the life cycle of an event as defined by the National Response Framework. Emergency response guidelines and policies determine the level and scale of notification. IPAWS brings the following capability to the National Response Framework:

3. To prevent and mitigate events through its alert and warning role
4. To provide reassurance and follow-up guidance in the response role
5. To focus messages to targeted and potential areas at risk

B.3 IPAWS Operational Concepts

The operational concept of the IPAWS incorporates and maintains the national-level EAS as a contingency system with its fundamental requirements intact. The President continues to have access to the EAS at all times, with the capability for activation within 10 minutes. Activation rests solely with the President, and EAS provides high probability that at least a portion of the total system would be available for Presidential use under the most severe circumstances. EAS will be able to transmit Information Programming and it continues to be able to preempt all other broadcast and cable programming. EAS, along with other emergency notification mechanisms, remains a part of the overall public alert and warning system over which FEMA exercises jurisdiction. IPAWS will incorporate and integrate these systems into a national-level alert and all-hazards warning system.

IPAWS requires a capability to process near-real-time weather and risk predictions to identify collaboratively-determined alert zones in order to enable geo-targeted alerting based on risks to specific homes, buildings, neighborhoods, cities, and regions via many last-mile means of message dissemination, such as telephones and other devices, such as cellular phones, pagers, desktop computers, sirens, electronic bulletin boards, FM data receivers, and other public information networks and devices.

Alert and warning content must also be delivered by people and technologies that translate English into an agreed upon number of non-English dialects (prioritized according to Census data) and leverage other non-language-based information presentation methods (i.e., sign language, flashing lights, sirens, hand-and-arm-signals).

B.4 IPAWS CAP v1.1 Profile - EAS Message Source and Target Descriptions

IPAWS will need to accept and/or apply some standard form of formatted message designed for emergency alerting and deliver the components needed for multiple message exchange partners. One of these partners is the EAS. However, the content of an incoming message or an IPAWS-generated alert defined herein (EAS “source”) must contain the components expected by all of the potential message exchange partners (each exchange partner is a “target”). For purposes of this document at this time the target is the FCC Part 11 message structures supporting EAS.

B.4.1 IPAWS CAP v1.1 Profile - EAS Description (Source)

By starting with the complete CAP v1.1 specification we can map the needs of the EAS FCC Part 11 message structure to the individual elements and attributes and further constrain the specification as well as add <parameter> tags for any unique needs of the EAS message that do not correspond to existing CAP elements. Figure 3 depicts the Document Object Model (DOM) of the CAP v.1.1 as defined verbatim by OASIS.

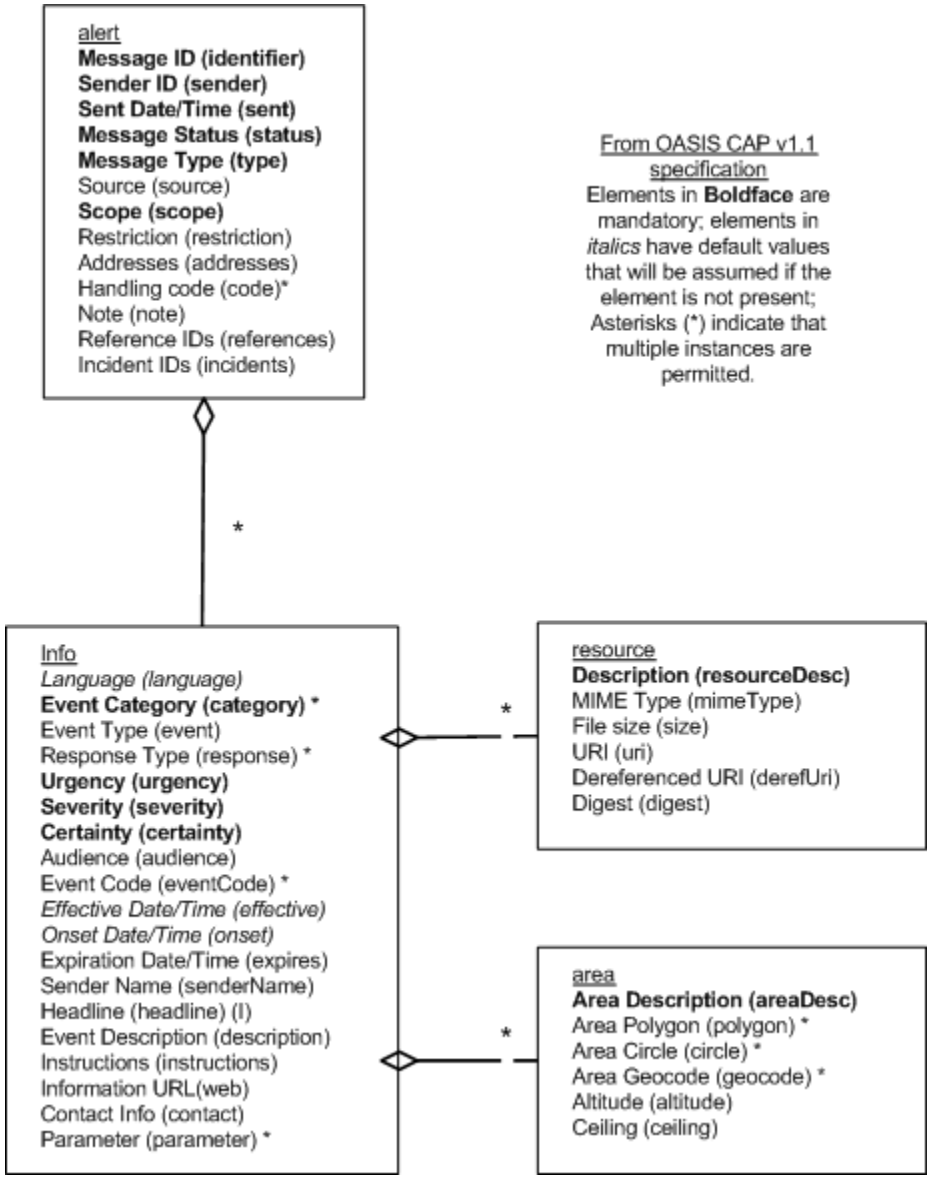


Figure 3- Document Object Model (DOM) of CAP v.1.1 as defined by OASIS

Requirements in following sections define the “source” Profile by tailoring and constraining CAP v1.1. The following excerpt is from “Common Alerting Protocol, v. 1.1 - OASIS Standard CAP-v1.1, October 2005,” providing general context for the Profile definition.

- **Interoperability** – First and foremost, the CAP Alert Message should provide a means for interoperable exchange of alerts and notifications among all kinds of emergency information systems.
- **Completeness** – The CAP Alert Message format should provide for all the elements of an effective public warning message.

- **Simple implementation** – The design should not place undue burdens of complexity on technical implementers.
- **Simple XML and portable structure** – Although the primary anticipated use of the CAP Alert Message is as an XML document, the format should remain sufficiently abstract to be adaptable to other coding schemes.
- **Multi-use format** – One message schema supports multiple message types (e.g., alert / update / cancellations / acknowledgements / error messages) in various applications (actual / exercise / test / system message.)
- **Familiarity** – The data elements and code values should be meaningful to warning originators and non-expert recipients alike.
- **Interdisciplinary and international utility** – The design should allow a broad range of applications in public safety and emergency management and allied applications and should be applicable worldwide.

The Common Alert Protocol SHOULD:

- Provide a specification for a simple, extensible format for digital representation of warning messages and notifications;
- Enable integration of diverse sensor and dissemination systems;
- Be usable over multiple transmission systems, including both TCP/IP-based networks and one-way "broadcast" channels;
- Support credible end-to-end authentication and validation of all messages;
- Provide a unique identifier (e.g., an ID number) for each warning message and for each message originator;
- Provide for multiple message types, such as:
  - Warnings
  - Acknowledgements
  - Expirations and cancellations
  - Updates and amendments
  - Reports of results from dissemination systems
  - Administrative and system messages
- Provide for multiple message types, such as:
  - Geographic targeting
  - Level of urgency
  - Level of certainty
  - Level of threat severity
- Provide a mechanism for referencing supplemental information (e.g., digital audio or image files, additional text);
- Use an established open-standard data representation;
- Be based on a program of real-world cross-platform testing and evaluation;
- Provide a clear basis for certification and further protocol evaluation and improvement; and, provide a clear logical structure that is relevant and clearly applicable to the needs of emergency response and public safety users and warning system operators.

B.4.2 Emergency Alert System (EAS) FCC CFR Title 47 Part 11 Description (Target)

For purposes of this document the “target” is the FCC Part 11 message structures supporting EAS.

From the FCC Part 11 – Emergency Alert System (EAS):

> *(a) The EAS is composed of broadcast networks; cable networks and program suppliers; AM, FM, Low Power FM (LPFM) and TV broadcast stations; Class A television (CA) stations; Low Power TV (LPTV) stations; cable systems; wireless cable systems which may consist of Multipoint Distribution Service (MDS), Multichannel Multipoint Distribution Service (MMDS), or Instructional Television Fixed Service (ITFS) stations; and other entities and industries operating on an organized basis during emergencies at the National, State and local levels. It requires that at a minimum all participants use a common EAS protocol, as defined in **§** 11.31, to send and receive emergency alerts…*

An EAS activation of a test or an alert consists of up to four elements:

1. A header code
2. An attention signal
3. An aural message
4. An end of message code

Complete technical specification of the mapping methodology intended between the IPAWS CAP v1.1 Profile and the EAS message structure are included below.

B.4.3 IPAWS CAP v1.1 Profile Structure Requirements

In order to meet the needs of the devices intended to receive alerts and warnings in a standard, recognized format, an IPAWS CAP v1.1 Profile will be developed to constrain the robust XML standard for simplicity and into a manageable size for meeting unique device and media requirements for transport and consumption.

The WC3 defines an XML Schema as follows:

> *An XML Schema is a description of a type of XML document, typically expressed in terms of constraints on the structure and content of that document type, above and beyond the basic syntactical constraints imposed by XML itself. AN XML Schema provides a view of a document type at a relatively high level of abstraction.*

An XML Profile is applied to an existing XML Schema (in this case the OASIS Standard CAP v1.1 Schema) in order to constrain or enforce aspects of it to accomplish a specific purpose according to the definition and criteria set forth for an XML Profile. Any message that is in compliance with the Profile must validate against the original XML Schema as well as the resulting XML Schema of the Profile.

CAP v1.1 is an XML message standard that also contains an XML Schema, which is to be used for validation of the CAP v1.1 message. A CAP v1.1 Profile (or any Standard Profile) MUST result in a constrained XML message adhering to the following requirements.

B. Table 1: CAP v1.1 Profile Criteria and Miscellaneous Requirements

CAP v1.1 Profile Criteria & Miscellaneous Requirements	
Number	**Requirement**
1.	A developed and agreed-to CAP v1.1 Profile and resulting Schema MUST adhere to the requirements contained herein.
2.	Unless otherwise stated within this "CAP v1.1 Profile Requirements" table, all OASIS CAP v1.1 elements SHALL be adhered to exactly as specified in the OASIS CAP v1.1 Standard.
3.	A CAP v1.1 Profile MUST not become a new or additional messaging "standard" (i.e., another Alerts and Warnings standard or another CAP v1.1 "version"). It is simply a more constrained version of an *existing* messaging standard.
4.	A CAP v1.1 Profile message MUST comply with the CAP v1.1 standard. • A CAP v1.1 Profile message MUST *always* validate against the CAP v1.1 standard Schema. Definition and Development of the IPAWS CAP v1.1 Profile message may or may not result in a more restrictive Schema. • A CAP v1.1 Profile message MUST validate within the CAP v1.1 standard namespace with no changes to root elements. • A CAP v1.1 Profile message MUST use all required elements (i.e., no deletion of required elements are allowed). • A CAP v1.1 Profile message MUST not change attributes for required fields.
5.	A CAP v1.1 Profile MUST be capable of using an existing CAP v1.1 standard service (i.e., software designed to apply the standard) to receive and understand an IPAWS CAP v1.1 Profile message, but an IPAWS CAP v1.1 Profile service may or may not be able to receive and understand a CAP v1.1 message.
6.	A CAP v1.1 Profile / message MUST NOT be Proprietary Format.
7.	A CAP v1.1 Profile message MAY further constrain the CAP standard.* (* may be thought of as a "constraint Schema" against the standard)
8.	A CAP v1.1 Profile message MAY add to required element definitions.* (* only to extend or interpret the definition)
9.	A CAP v1.1 Profile message MAY limit the size of required elements.
10.	A CAP v1.1 Profile message MAY exclude optional elements.
11.	A CAP v1.1 Profile MAY define elements in a specific, agreed-upon way – as defined and adjudicated for the Profile.

B.5 IPAWS CAP v1.1 Profile Methodology & Requirements

As summarized earlier, the <alert> block of the CAP v1.1 message will be utilized by IPAWS to determine routing, handling and combined security level identification. The <alert> block is not specific to any included <info> block, but a general reference to all associated <info> blocks and their content. No specific information about any particular <info> block will be included in the <alert> block, unless it will not impact any subsequent <info> blocks. The <alert> block is designed for IPAWS general use. Each <info> block is designed to meet the needs of individual message exchange partners.

The methodology applied while proceeding through the CAP v1.1 elements list gives preference to EAS for each element interrogated. As future exchange partners are added and conflicts arise (i.e., if an element is used for a purpose specific to a particular exchange partner), CAP extensions must be added using the <parameter> element, which may duplicate the intent of some of the <alert> elements.

Figure 4 presents the required IPAWS CAP v1.1 Profile Model with EAS-specific components demonstrating the <parameter> concept. Figure 4 is followed by Table 1: "IPAWS Profile <alert> block," providing the requirements and guidelines of the elements that are in common and that are intended to apply to all potential message exchange partners. Subsequent tables provide the requirements and guidelines for the elements that are exchange partner-specific (EAS-specific for this document at this time).

Unless otherwise stated within these tables, all OASIS CAP v1.1 elements SHALL be adhered to exactly as specified in the OASIS CAP v1.1 Standard. Terminology within these tables SHALL be interpreted in accordance with Request for Comments (RFC) 2119. "Shall" and "Must" represent absolute requirements, while other terminology represents guidelines or instructions. Where the "Non-Conformance Impact" is blank no impact applies.

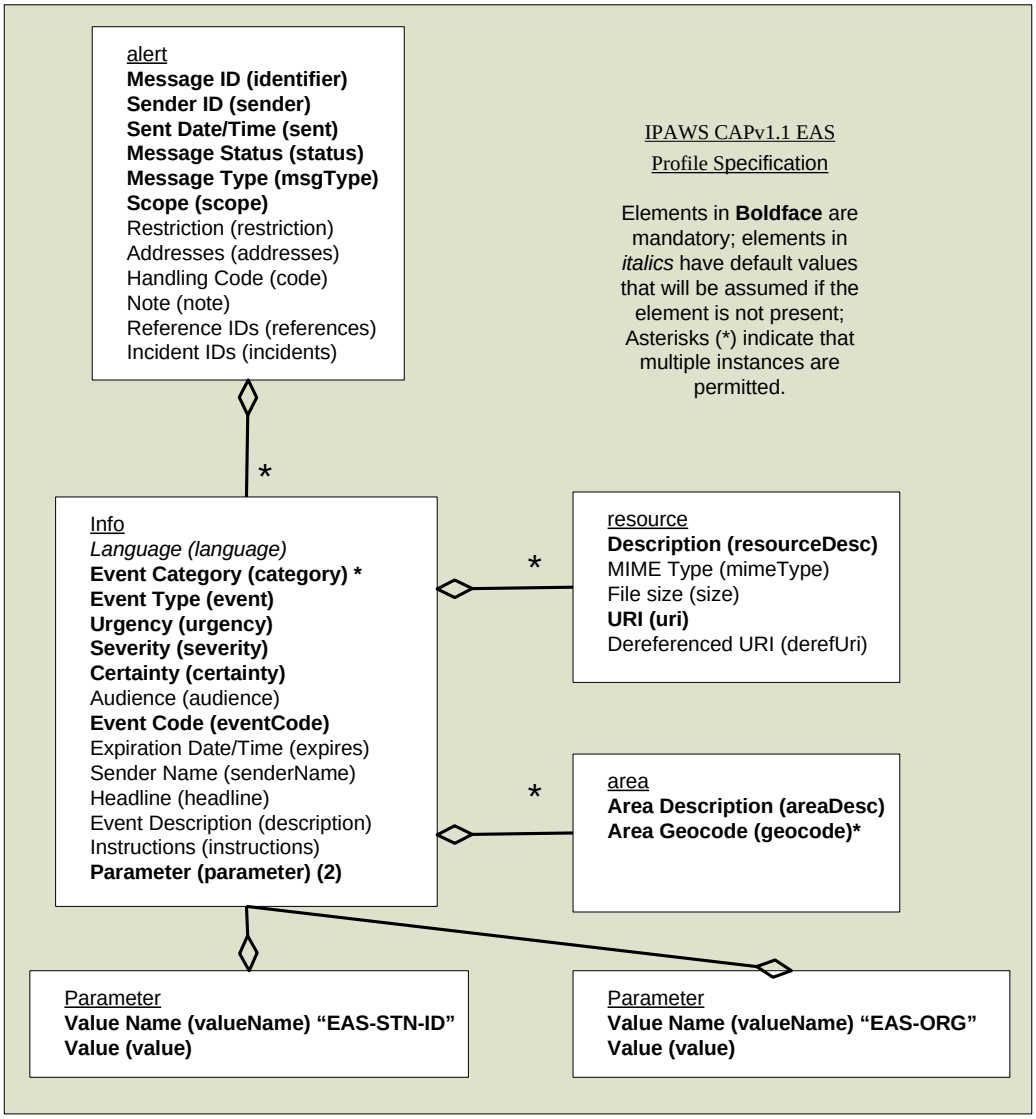


Figure 4- Required IPAWS CAP v1.1- Profile Model with EAS specific information

B.5.1 IPAWS CAP v1.1 Profile Common Elements

Table 1 represents the requirements and guidelines for the <alert> block of the IPAWS CAP v1.1 Profile that are intended to apply to all potential message exchange partners.

B. Table 2: IPAWS CAP v1.1 EAS Profile <alert> block Requirements

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
<alert>	**The container for all component parts of the alert message (REQUIRED)**	This element MUST: (1) Surround CAP alert message sub-elements (2) include the xmlns attribute referencing the CAP URN as the namespace, e.g.: <cap:alert xmlns:cap="urn:oasis:names:tc:emergency:cap:1.1"> *[sub-elements]* </cap:alert> (3) In addition to the specified sub-elements, MAY contain one or more <info> blocks, each specific to only one identified message exchange partner (e.g. EAS, CMAS, HazCollect).	The message will be discarded by IPAWS as non-compliant. Schema validation will fail.
<identifier>	**The identifier of the alert message (REQUIRED)**	This element MUST: (1) Contain a number or string uniquely identifying this message, assigned by the sender. (2) MUST NOT include spaces, commas or restricted characters (< and &). *Note: Applies to the entire message, not individual <info> blocks.*	If <identifier> does not exist, the message SHALL be ignored; if invalid, the message SHALL be rejected. The message will be discarded by IPAWS as non-compliant. Schema validation will fail.
<sender>	**The identifier of the sender of the alert message** **(REQUIRED)**	This element MUST: (1) Identify the originator of this alert. Guaranteed by assigner to be unique globally; e.g., may be based on an Internet domain name (2) MUST NOT include spaces, commas or restricted characters (< and	If <sender> does not exist, the message SHALL be ignored; if invalid, the message SHALL be rejected.

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
		&).	The message will be discarded by IPAWS as non-compliant. Schema validation will fail.
<sent> **Used for EAS Header Code assembly per the Technical Specifications.**	**The time and date of the origination of the alert message (REQUIRED)**	This element MUST: (1) Include the date and time represented in **[dateTime]** format (e. g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT). (2) Alphabetic time zone designators such as “Z” MUST NOT be used. The time zone for UTC MUST be represented as “-00:00” or “+00:00.” *Note: Applies to the entire message, not individual <info> blocks.*	If <sent> does not exist, the message SHALL be ignored; if invalid, the message SHALL be rejected. The message will be discarded by IPAWS as non-compliant. Schema validation will fail. Must be converted to EAS **JJJHHMM** Effective Date/Time. If cannot be converted due to missing time zone or a syntax error then message SHALL be rejected.
<status>	**The code denoting the appropriate handling of the alert message (REQUIRED)**	This element MUST: Contain one of the following Code Values: “Actual” - Actionable by all targeted recipients “Exercise”- Actionable only by designated exercise participants; exercise identifier should appear in <note> “System” - For messages that support alert network internal functions. “Test” - Technical testing only, all recipients disregard “Draft” – A preliminary template or draft, not actionable in its current form. In the use of EAS: EAS Event Codes DMO, NMN, NPT, RMT, and RWT	If <sent> does not exist, the message SHALL be ignored; if invalid, the message SHALL be rejected. The message will be discarded by IPAWS as non-compliant. Schema validation will

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
		SHALL set the <status> to “Actual”. Messages with a CAP <status> element <value> of “Test” will not be rendered to an EAS broadcast message. All <info> blocks MUST be of the same status type.	fail.
<msgType>	**The code denoting the nature of the alert message (REQUIRED)**	This element MUST: Contain one of the following Code Values: “Alert” - Initial information requiring attention by targeted recipients “Update” - Updates and supersedes the earlier message(s) identified in <references> “Cancel” - Cancels the earlier message(s) identified in <references> “Ack” - Acknowledges receipt and acceptance of the message(s)) identified in <references>; explanation should appear in <note> preceded by “Ignored:”, “Accepted:”, or “Aired on:”, as appropriate. “Aired on” shall be followed by the FCC Call Sign(s) of the station(s) on which the alert was broadcast. “Error” indicates rejection of the message(s) identified in <references>; explanation SHOULD appear in <note> preceded by “Error:” *Note: Must apply to all <info> blocks in the message. Multiple “Ack” messages may be necessary in cases where multiple broadcast outlets are processed through the same receiving equipment.*	If <msgType> does not exist, the message SHALL be ignored; if invalid, the message SHALL be rejected. The message will be discarded by IPAWS as non-compliant. Schema validation will fail.
<scope>	**The code denoting the intended distribution of the alert message (REQUIRED)**	This element MUST: Contain one of the following Code Values: “Public” - For general dissemination to unrestricted audiences “Restricted” - For dissemination only to users with a known operational requirement (see <restriction>, below) “Private” - For dissemination only to specified addresses (see <address>, below). When any info.audience block (described below) sets an Executive Order 12958 classification level *to Confidential, Secret or Top Secret* the <scope> MUST be set to “Restricted” or “Private” and the highest level of Combined Confidentiality of all info.audience elements will be reflected in the <restriction> element as described below.	If <scope> does not exist, the message SHALL be ignored; if invalid, the message SHALL be rejected. The message will be discarded by IPAWS as non-compliant. Schema validation will fail.

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
<restriction>	The text describing the rule for limiting distribution of the restricted alert message Used when <scope> is set to “Private” or “Restricted” (CONDITIONAL)	If condition is met, this element MUST: 1. Reflect the combined classification of all of the <info> blocks. Set in accordance with Executive Order 12958: *Unclassified, Confidential, Secret or Top Secret* 2. Reflect the combination of any data that may result in a higher security classification 3. Be equal to or higher than any info.audience classification as described below 4. Apply to the handling of the entire message. *Note: When <scope> is “Private”, <restriction> Is to be used as a combined confidentiality marker for all <info> blocks. This method allows messages marked as “Private” to be encrypted for secure delivery.*	If <scope> is “Private” or “Restricted” and <restriction> is empty, or not applied <restriction> will be assumed to be “Unclassified.”
<addresses>	The group listing of intended recipients of the private alert message (CONDITIONAL)	If condition is met, this element MUST: (1) Be used when <scope> value is "Private" (2) Identify each recipient by a unique identifier or address. (3) Enclose addresses including whitespace in double-quotes. Multiple space-delimited addresses MAY be included.	If <scope> is “Private” and <addresses> is empty, or not applied the message will be discarded by IPAWS as non-compliant. Schema validation will fail.
<code>	The code denoting the special handling of the alert message (OPTIONAL)	(1) Any user-defined flag or special code used to flag the alert message for special handling. (2) Multiple instances MAY occur within a single <info> block. Use to indicate originator-assured compliancy with the IPAWS CAP v1.1 Profile or future revisions. “IPAWSPv1.1” denotes the IPAWS CAP v1.1 Profile.	
<note>	The text describing the purpose or significance of the alert message	The message note is primarily intended for use with Cancel, Ack, and Error alert message types.	

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
	(OPTIONAL)		
<references>	The group listing identifying earlier message(s) referenced by the alert message (OPTIONAL)	If used, the element MUST: (1) Extend message identifier(s) (in the form *sender, identifier, sent)* of an earlier CAP message or messages referenced by this one. (2) Separate multiple messages by whitespace. The <references> list is to include the entire update trail and not just the most recent update.	
<incidents>	The group listing naming the referent incident(s) of the alert message (OPTIONAL)	(1) Used to collate multiple messages referring to different aspects of the same incident (2) If multiple incident identifiers are referenced, they SHALL be separated by whitespace. Incident names including whitespace SHALL be surrounded by double-quotes.	

B.5.2 IPAWS CAP v1.1 Profile EAS Specific Elements

The remaining tables represent the requirements and guidelines to create the EAS Profile <info> and other blocks of the IPAWS CAP v1.1 Profile which are intended to be EAS-specific. General guidelines for message creation of an EAS <info> block are defined below:

1. Conventions regarding case-sensitivity: XML specifications require that all CAP v1.1 element names MUST be case sensitive. Except where explicitly noted, <valueName> and <value> content are not case sensitive.
2. Conventions regarding Event Codes: All values for EAS Event Code SHALL be passed through by EAS devices, even if the Event Code is not shown in FCC Part 11.31, as long as the value is a three-letter code. This acknowledges the possible existence of non-Part 11 codes which appear in a State EAS Plan and are approved for special use by the FCC. Every effort SHOULD be used to implement EAS Event Codes as define below:

B. Table 3:FCC Approved Event Codes

Emergency Action Notification	EAN	Emergency Action Termination	EAT
National Information Center	NIC	National Periodic Test	NPT
Required Monthly Test	RMT	Required Weekly Test	RWT
Tornado Watch	TOA	Tornado Warning	TOR
Severe Thunderstorm Watch	SVA	Severe Thunderstorm Warning	SVR
Severe Weather Statement	SVS	Special Weather Statement	SPS
Flash Flood Watch	FFA	Flash Flood Warning	FFW
Flash Flood Statement	FFS	Flood Watch	FLA
Flood Warning	FLW	Flood Statement	FLS
Winter Storm Watch	WSA	Winter Storm Warning	WSW
Blizzard Warning	BZW	High Wind Watch	HWA
High Wind Warning	HWW	Evacuation Immediate	EVI
Civil Emergency Message	CEM	Practice/Demo Warning	DMO
Hurricane Statement	HLS	Hurricane Watch	HUA
Administrative Message	ADR	Hurricane Warning	HUW
Child Abduction Emergency	CAE	Civil Danger Warning	CDW
Earthquake Warning	EQW	Fire Warning	FRW
Hazardous Materials Warning	HMW	Law Enforcement Warning	LEW
Local Area Emergency	LAE	911 Telephone Outage Emergency	TOE
Radiological Hazard Warning	RHW	Shelter in Place Warning	SPW

B. Table 4: IPAWS CAP v1.1 Profile EAS <info> block Requirements

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
<info>	The container for all component parts of the info sub-element for the EAS Profile of the alert message **(REQUIRED)**	All content intended for EAS broadcast SHALL be placed in a single CAP v1.1<info> block within an Alert, and in the first <area> block within that <info> block. *Note: <info> blocks will be specifically tagged with <parameter> information as to which exchange partner is applicable to that block. The order in which the exchange partner <info> blocks appear in the <alert> is not constrained.*	Translator layer to EAS exchange partners will ignore all additional <info> and/or <area> blocks in an EAS CAP v1.1 message, which may result in loss of intended information.
<language>	The code denoting the language of the info sub-element of the alert message (OPTIONAL)	If used, this element MUST use: (1) Code Values: Natural language identifier per **[RFC 3066].** (2) If not present, an implicit default value of "en-US" SHALL be assumed. (3) A null value in this element SHALL be considered equivalent to "en-US." *Note: Multiple language usage is not defined in this version of the IPAWS CAP v1.1 Profile.*	
<category>	**The code denoting the category of the subject event of the alert message (REQUIRED)**	This element MUST contain one of the following: (1) Code Values: "Geo" - Geophysical (inc. landslide) "Met" - Meteorological (inc. flood) "Safety" - General emergency and public safety "Security" - Law enforcement, military, homeland and local/private security "Rescue" - Rescue and recovery "Fire" - Fire suppression and rescue "Health" - Medical and public health "Env" - Pollution and other environmental "Transport" - Public and private transportation "Infra" - Utility, telecommunication, other non-transport infrastructure "CBRNE" – Chemical, Biological, Radiological, Nuclear or High-Yield Explosive threat or attack "Other" - Other events (2) Multiple instances MAY occur within an EAS <info> block.	
<event>	**The text denoting**	The full text, or at least the first ten words, of this element will be used in	

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
Used for assembly of EAS recorded audio, EAS text-to-speech audio, and EAS video display text per the Technical Specifications.	**the type of the subject event of the alert message (REQUIRED)**	the construction of EAS recorded audio or EAS text-to-speech audio. The full text, or at least the first 60 characters, of this element will be used in the construction of EAS video display text.	
<urgency>	**The code denoting the urgency of the subject event of the alert message (REQUIRED)**	(1) The “urgency”, “severity”, and “certainty” elements collectively distinguish less emphatic from more emphatic messages (2) Code Values: “Immediate” - Responsive action SHOULD be taken immediately “Expected” - Responsive action SHOULD be taken soon (within next hour) “Future” - Responsive action SHOULD be taken in the near future “Past” - Responsive action is no longer required “Unknown” - Urgency not known EAS Event Codes DMO, NMN, NPT, RMT, and RWT SHALL set the <urgency> element value to “Unknown” *Note: CAP to EAS translation does not use this field.*	
<severity>	**The code denoting the severity of the subject event of the alert message (REQUIRED)**	(1) The “urgency”, “severity”, and “certainty” elements collectively distinguish less emphatic from more emphatic messages (2) Code Values: “Extreme” - Extraordinary threat to life or property “Severe” - Significant threat to life or property “Moderate” - Possible threat to life or property “Minor” - Minimal threat to life or property “Unknown” - Severity unknown. EAS Event Codes DMO, NMN, NPT, RMT, and RWT SHALL set the <severity> element value to “Minor.” *Note: CAP to EAS translation does not use this field*	
<certainty>	**The code denoting**	(1) The “urgency”, “severity”, and “certainty” elements collectively	

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
	the certainty of the subject event of the alert message (REQUIRED)	distinguish less emphatic from more emphatic messages. (2) Code Values: “Observed” – Determined to have occurred or to be ongoing. “Likely” - Likely (p > ~50%) “Possible” - Possible but not likely (p <= ~50%) “Unlikely” - Not expected to occur (p ~ 0) “Unknown” - Certainty unknown (3) For backward compatibility with CAP 1.0, the deprecated value of “Very Likely” SHOULD be treated as equivalent to “Likely.” EAS Event Codes DMO, NMN, NPT, RMT, and RWT SHALL set the <certainty> element value to “Unknown”. *Note: CAP to EAS translation does not use this field.*	
<audience>	The text describing the intended audience of the alert message (OPTIONAL)	If used, this element MUST be set to reflect the classification of the information contained in the <info> block. Set in accordance with Executive Order 12958: *Unclassified, Confidential, Secret or Top Secret.*	If missing “Unclassified” is assumed.
<eventCode> **Used for EAS Header Code assembly per the Technical Specifications.**	**A system-specific code identifying the event type of the alert message (REQUIRED)**	(1) Any system-specific code for event typing, in the form: <eventCode> <valueName>valueName</valueName> <value>value</value> </eventCode> Where the content of “valueName” is a user-assigned string designating the domain of the code, and the content of “value” is a string (which may represent a number) denoting the value itself (e.g., valueName ="SAME" and value="CEM"). (2) Values of “valueName” that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP). The EAS <eventCode> <valueName> must be “SAME”. The EAS <eventCode> <value>, such as CAE or CEM, is case-sensitive and SHALL be a 3-letter alphabetic code.	If <eventCode> does not exist, the message SHALL be ignored; if invalid, the message SHALL be rejected. Message rejected by Translator.

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
		Only one <eventCode> is allowed in the EAS <info> block. *Notes: Any EAS Event Code may be sent with a CAP <status> element <value> of "Test", in which case that alert SHALL not be broadcast as a valid alert but treated as a log-only event.* *All values for EAS Event Code SHALL be passed through by EAS CAP Profile devices, even if the Event Code is not shown in FCC Part 11.31, as long as the value is a three-letter code. This acknowledges the possible existence of non-Part 11 codes which appear in a State EAS Plan and are approved for special use by the FCC.*	
<expires> **Used for EAS Header Code assembly per the Technical Specifications.**	The expiry time of the information of the alert message (OPTIONAL)	(1) The date and time is represented in **[dateTime]** format (e. g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT). (2) Alphabetic time zone designators such as "Z" MUST NOT be used. The time zone for UTC MUST be represented as "-00:00" or "+00:00." While the ISO 8601 format considers indication of Time Zone to be optional, the <info><expires> element SHOULD include a Time Zone.	If the optional <expires> field is missing, the expired time will be assumed to be one hour greater than the <sent> element. That is, 0100 shall be assumed for the EAS Duration (TTTT). If there are no other errors, the message SHALL be accepted.
<senderName> **Used for assembly of EAS recorded audio, EAS text-to-speech audio, and EAS video display text per the Technical Specifications.**	The text naming the originator of the alert message (OPTIONAL)	The human-readable name of the agency or authority issuing this alert. The full text, or at least the first ten words, of this element will be used in the construction of EAS recorded audio or EAS text-to-speech audio. The full text, or at least the first 60 characters, of this element will be used in the construction of EAS video display text.	If <senderName> is not included the EAS translator will utilize the words "Emergency Alert System"
<headline>	The text headline of the alert message	A brief human-readable headline. Note that some displays (for example, short messaging service devices) may only present this headline; it	

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
Used for assembly of EAS recorded audio, EAS text-to-speech audio, and EAS video display text per the Technical Specifications.	(OPTIONAL)	SHOULD be made as direct and actionable as possible while remaining short. 160 characters MAY be a useful target limit for headline length. The full text, or at least the first ten words, of this element will be used in the construction of EAS recorded audio or EAS text-to-speech audio. The full text, or at least the first 60 characters, of this element will be used in the construction of EAS video display text.	
<description> **Used for assembly of EAS recorded audio, EAS text-to-speech audio, and EAS video display text per the Technical Specifications.**	(OPTIONAL)	An extended human readable description of the hazard or event that occasioned this message. The full text, or at least the first one hundred words, of this element will be used in the construction of EAS recorded audio or EAS text-to-speech audio. The full text, or at least the first 900 characters, of this element will be used in the construction of EAS video display text.	
<instruction> **Used for assembly of EAS recorded audio, EAS text-to-speech audio, and EAS video display text per the Technical Specifications.**	(OPTIONAL)	An extended human readable instruction to targeted recipients. (If different instructions are intended for different recipients, they should be represented by use of multiple <info> blocks.) The full text, or at least the first one hundred words, of this element will be used in the construction of EAS recorded audio or EAS text-to-speech audio. The full text, or at least the first 900 characters, of this element will be used in the construction of EAS video display text.	
<parameter> (EAS-ORG) **Used for EAS**	**A system-specific additional parameter associated with the**	(1) Any system-specific datum, in the form: <parameter> <valueName>valueName</valueName> <value>value</value>	Message rejected by Translator. If this optional field is not present, processing

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
Header Code assembly per the Technical Specifications.	**alert message (Optional)**	</parameter> where the content of “valueName” is a user-assigned string designating the domain of the code, and the content of “value” is a string (which may represent a number) denoting the value itself (e.g., valueName ="SAME" and value="CIV".) (2) Values of “valueName” that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP). The EAS Originator Code (ORG) SHALL be included in the <value> element with a <valueName> of “EAS-ORG”. The EAS-ORG <value>, such as EAS or PEP, is case-sensitive and SHALL be a 3-letter alphabetic code. Only one EAS-ORG <parameter> is allowed in the EAS <info> block.	devices SHALL assume that the originator is CIV, and if there are no other errors, the message SHALL be accepted.
<parameter> (EAS-STN-ID) **Used for EAS Header Code assembly per the Technical Specifications.**	**A system-specific additional parameter associated with the alert message (OPTIONAL)**	(1) Any system-specific datum, in the form: <parameter> <valueName>valueName</valueName> <value>value</value> </parameter> where the content of “valueName” is a user-assigned string designating the domain of the code, and the content of “value” is a string (which may represent a number) denoting the value itself (e.g., valueName ="SAME" and value="CIV".) (2) Values of “valueName” that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP). The EAS STATION ID (LLLLLLLL) SHALL be included in the <value> element with a <valueName> of “EAS-STATION-ID”. The EAS-STATION-ID <value> is case-sensitive and SHALL be up to 8 printable characters, but cannot be a dash '-' or plus '+' character. Only one EAS-STATION-ID <parameter> is allowed in the EAS <info> block.	Message rejected by Translator. If this optional field is not present, processing devices may create the EAS STATION ID as 8 space characters or some other system-defined value.
<parameter>	A system-specific	(1) Any system-specific datum, in the form:	If this parameter is not

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
(EAS-Must-Carry) **Used for EAS Header Code assembly per the Technical Specifications.**	additional parameter associated with the alert message (CONDITIONAL)	<parameter> <valueName>valueName</valueName> <value>value</value> </parameter> where the content of “valueName” is a user-assigned string designating the domain of the code, and the content of “value” is a string (which may represent a number) denoting the value itself (e.g., valueName ="SAME" and value="CIV".) (2) Values of “valueName” that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP). If this parameter is present and the value is TRUE, then the CAP message has come from a state governor’s office and the EAS system must place the message on air with priority status.	present or the value is FALSE, then the CAP message has not come from a state governor’s office and the EAS system is not *required* to process the message with priority status.

Table 5: IPAWS CAP v1.1-EAS Profile <info><resource> block Requirements

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
<resource>	The container for all component parts of the <resource> sub-element of the <info> sub-element of the <alert> element **(CONDITIONAL)**	(1) Refers to an additional file with supplemental information related to this <info> element; e.g., an image or audio file (2) Multiple occurrences MAY occur within a single <info> block	No audio processing can/will occur if <resource> is not included.
<resourceDesc> **Used for assembly of EAS recorded audio, EAS**	**The text describing the type and content of the resource file** **(CONDITIONAL)**	The human-readable text describing the content and kind, such as “map” or “photo,” of the resource file. If <resource> is used <resourceDesc> MUST be defined as follows where applicable:	If <info><resource> exists and <resourceDesc> does not exist, the message SHALL be ignored; if invalid, the message

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
streaming audio, and EAS text-to-speech audio per the Technical Specifications.		“EAS Audio” (for recorded audio file attachment) “EAS Streaming Audio” (for streaming audio URI).	SHALL be rejected.
<mimeType>	The identifier of the MIME content type and sub-type describing the resource file (OPTIONAL)	MIME content type and sub-type as described in [RFC 2046]. (As of this document, the current IANA registered MIME types are listed at http://www.iana.org/assignments/mediatypes/)	
<size>	The integer indicating the size of the resource file (OPTIONAL)	Approximate size of the resource file in bytes.	
<uri> **Used for assembly of EAS recorded audio, EAS streaming audio, and EAS text-to-speech audio per the Technical Specifications.**	The identifier of the hyperlink for the resource file (**CONDITIONAL**)	A full absolute URI, typically a Uniform Resource Locator that can be used to retrieve the resource over the Internet OR a relative URI to name the content of a <derefUri> element if one is present in this resource block.	If <info><resource> exists and <uri> does not exist, the message SHALL be ignored; if invalid, the message SHALL be rejected.
<drefUri>	The base-64 encoded data content	(1) MAY be used either with or instead of the <uri> element in messages transmitted over one-way (e.g., broadcast) data links where retrieval of a	

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
	of the resource file (CONDITIONAL)	resource via a URI is not feasible. (2) Clients intended for use with one-way data links MUST support this element. (3) This element MUST NOT be used unless the sender is certain that all direct clients are capable of processing it. (4) If messages including this element are forwarded onto a two-way network, the forwarder MUST strip the <derefUri> element and SHOULD extract the file contents and provide a <uri> link to a retrievable version of the file. (5) Providers of one-way data links MAY enforce additional restrictions on the use of this element, including message-size limits and restrictions regarding file types. Needed if alert data is sent within message.	

B. Table 6: IPAWS CAP v1.1 Profile - EAS <info><area> block Requirements

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
<area>	The container for all component parts of the <area> sub-element of the <info> sub-element of the <alert> message (OPTIONAL)	(1) Multiple occurrences permitted, in which case the target area for the <info> block is the union of all the included <area> blocks. (2) MAY contain one or multiple instances of <polygon>, <circle> or <geocode>. If multiple <polygon>, <circle> or <geocode> elements are included, the area described by this <area> is the union of those represented by the included elements. If element is used, only the first <info><area> block is allowed for EAS Processing. Basic syntax example:	Additional <area> blocks beyond the first attached to an EAS <info> block will be ignored. The presence of more than one area block SHALL NOT cause the message to be rejected or ignored.

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
		<area> <areaDesc>Arlington, VA</areaDesc> <geocode> <valueName>SAME</valueName> <value>022292</value> </geocode> </area>	
<areaDesc> **Used for assembly of EAS recorded audio, EAS text-to-speech audio, and EAS video display text per the Technical Specifications.**	**The text describing the affected area of the alert message** **(REQUIRED)**	A text description of the affected area. If <info><area> is used than <areaDesc> is required. The full text, or at least the first one hundred words, of this element will be used in the construction of EAS recorded audio or EAS text-to-speech audio. The full text, or at least the first 900 characters, of this element will be used in the construction of EAS video display text.	If <info><area> exists and <areaDesc> does not exist, the message SHALL be ignored; if invalid, the message SHALL be rejected.
<geocode> **Used for EAS Header Code assembly per the Technical Specifications.**	**The geographic code delineating the affected area of the alert message** **(REQUIRED)**	(1) Any geographically-based code to describe message target area: <parameter> <valueName>valueName</valueName> <value>value</value> </parameter> where the content of “valueName” is a user-assigned string designating the domain of the code, and the content of “value” is a string (which may represent a number) denoting the value itself (e.g., valueName ="SAME" and value="006113"). (2) Values of “valueName” that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP).	If <info><area> exists and <geocode> does not exist, the message SHALL be ignored; if invalid, the message SHALL be rejected. If <geocode> does not have <valueName> of “SAME” it will be ignored. If the <value> is not in PSSCCC format it will be

Element/Attribute or Content	Definition and Optionality	Requirement	Non-Conformance Impact
		(3) Multiple instances MAY occur within a single <info> block. (4) This element is primarily for compatibility with other systems. Use of this element presumes knowledge of the coding system on the part of recipients; therefore, for interoperability, it SHOULD be used in concert with an equivalent description in the more universally understood <polygon> and <circle> forms whenever possible. This element MUST contain at least one <geocode> with <valueName> of “SAME” and one <value> string representing the 6-digit EAS Location code (**PSSCCC),** defined per CFR 47 Part 11. Example: <geocode> <valueName>SAME</valueName> <value>006013</value> </geocode> A location code consisting of all zeros ("000000") shall indicate a message intended for the entire United States and Territories.	rejected.

B.6 IPAWS CAP v1.1 Profile EAS Technical Specifications

The purpose of this section is to provide a technical specification for equipment manufacturers for translation FROM a message constructed in accordance with the IPAWS CAP v1.1 Profile TO the FCC Part 11 target message formats. Construction of an EAS message consumable by an EAS device in accordance with the IPAWS CAP v1.1 Profile requires logic in the translation layer. The following documentation is presented in the form of detailed flowcharts which start with the incoming IPAWS CAP v1.1 message, step through the translation process, and result in an EAS alert.

EAS Decoder specifications can be found in the Electronic Code of Federal Regulations Part 11.33: (http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr;rgn=div8;view=text;node=47%3A1.0.1.1.11.2.237.3;idno=47;cc=ecfr)

An EAS activation of a test or an alert consists of up to four elements:

1. A header code. **All** EAS activations will include a header code data burst. The header code will be sent three times, with a one-second pause after each transmission, to ensure proper reception by EAS devices.
2. An attention signal. Following the header code, a two-tone attention signal is used to alert listeners and viewers that EAS activation has occurred and that a message will follow. The attention signal should be used if, and only if, a message will be included as part of the alert.
3. A message. The message may be audio, video, or text. The message follows the attention signal. Use of the two-tone attention signal and a message will be determined by the originator of the alert; they are not required, but if one is used the other MUST accompany it.
4. An end of message code. **All** EAS activations will conclude with an end-of-message code data burst. The end-of- message code will be sent three times, with at least a one-second pause after each transmission, to ensure proper reception by EAS devices.

Figure 5 is a depiction of the general translation logic, followed by specific sections for the construction of audio, text-to-speech, audio, and video display text.

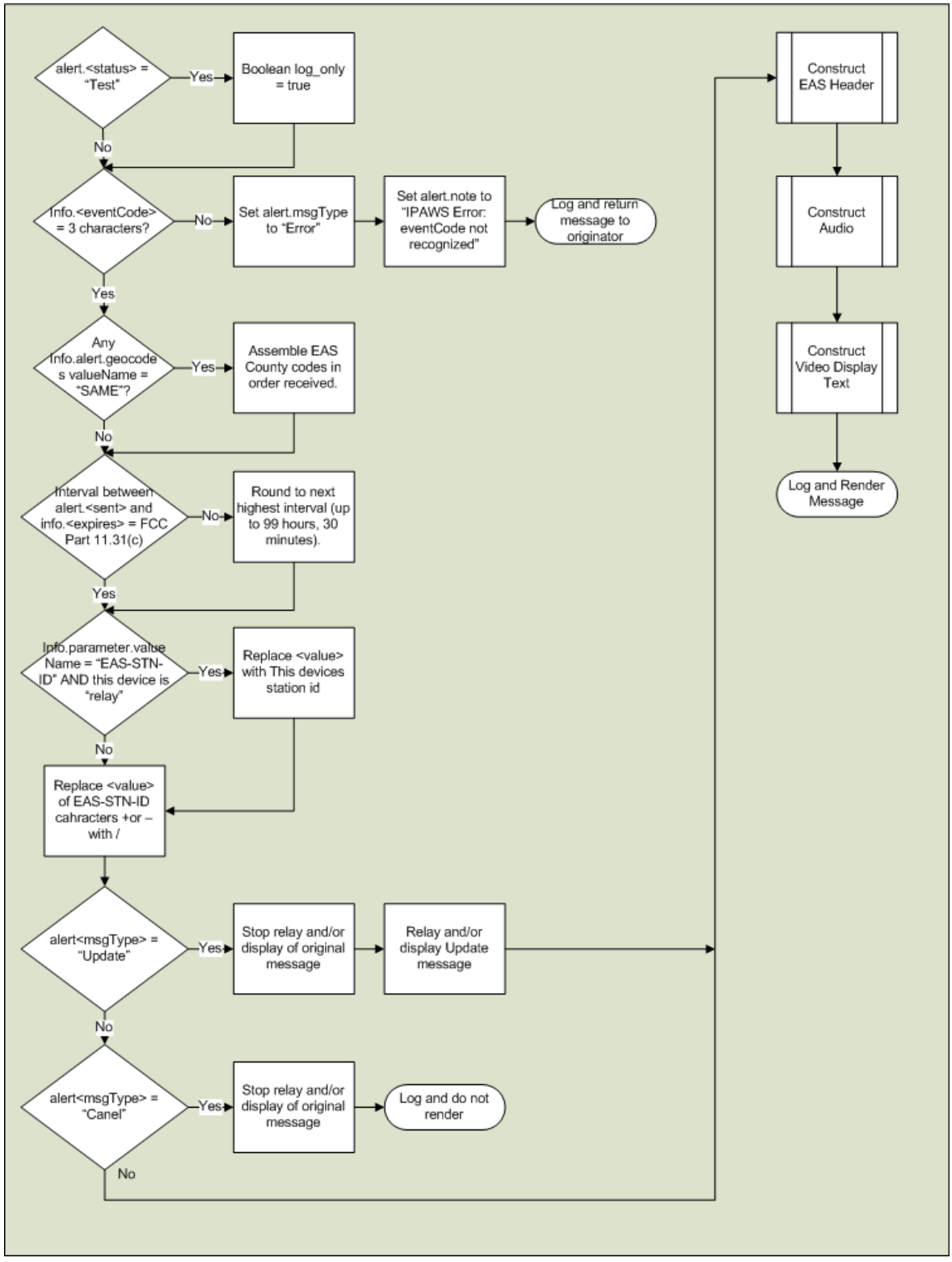


Figure 5- General EAS Processing

3.5 Constructing an EAS Header Code from IPAWS CAP v1.1 Profile

The FCC Part 11.31c specifies that EAS Header Codes consist of the following elements sent the in the following sequence:

[Preamble] ZCZC-ORG-EEE-PSSCCC+TTTT-JJJHHMM-LLLLLLLL

IPAWS CAP v1.1 Profile elements will be used in the construction of the EAS Header as follows:

- The [Preamble] clears the system and is sent automatically by the EAS encoder.
- The identifier (**ZCZC**) indicates the start of the American Standard Code for Information Interchange (ASCII) code and is sent automatically by the EAS encoder.
- The EAS Originator Code (ORG) describes the type of entity originating an EAS activation. It is programmed into an EAS encoder by the user at initial setup. The EAS Originator Code (ORG) SHALL be included in the <value> element of a CAP <info><parameter> block with a <valueName> of “EAS-ORG”. Originator Codes are specified in FCC Part 11.31d, as follows. Though not specified in FCC Part 11.31d, “EAN” is included as a reserved EAS Originator Code for future means of transmitting messages for EAN events.
    - **EAN** - Emergency Action Notification
    - **PEP** - Primary Entry Point System
    - **EAS** - Broadcast station or cable system
    - **WXR** - National Weather Service
    - **CIV** - Civil authorities
- The EAS Event Code (EEE) describes the type of event that has occurred and must be programmed into an encoder by the originator for each activation. The EEE SHALL be represented using the CAP <info><eventCode> element with a <valueName> of “SAME.”
    - The EEE <value>, such as CAE or CEM, is case sensitive.
    - Note that in some cases, such as tests, the encoder may use a macro function which assigns the event code, making it seem like no Event Code was specified.
- Each EAS County Location Code (PSSCCC) SHALL be included in the <value> element of a separate CAP <area><geocode> element with a <valueName> of “SAME.”
    - This <value> is understood to be the 6-digit EAS/SAME Location Code, comprised of the standard FIPS Code with a leading digit indicating the 1/9th area sub-division.

- The geocodes SHALL be placed into the EAS ZCZC string in the order that they are encountered in the CAP message. This is required to allow duplicate EAS messages to be detected.
- A location code consisting of all zeros ("000000") shall indicate a message intended for the entire United States and Territories.

- The EAS Duration (TTTT) SHALL be represented using the CAP <info><expires> element in the International Organization for Standardization (ISO) 8601 format per the OASIS CAP 1.1 specification.
  - The interval between the CAP <alert><sent> and <info><expires> elements SHOULD be one of the intervals permitted for the “TTTT” parameter in FCC Part 11.31(c).
  - If the interval between <sent> and <expires> elements is less than one hour, the valid range permitted for EAS Duration shall be 0015, 0030, or 0045.
  - If the interval between <sent> and <expires> elements is greater than one hour, the valid range permitted for EAS Duration shall be in half-hour increments from 0100 to 9930.
  - If a message is received with an interval between the <sent> and <expires> elements that does not conform to one of the intervals permitted for the “TTTT” parameter in FCC Part 11.31(c)., the interval shall be rounded to the next highest permitted interval up to 99 hours, 30 minutes. FCC Part 11 did not place an upper limit on EAS Duration, allowing a value of 9930.
- The EAS Time Alert Issued (JJJHHMM) SHALL be represented using the CAP <alert><sent> element in the ISO 8601 format per the OASIS CAP 1.1 specification.
- The EAS Station ID (LLLLLLLL) SHALL be included in the <value> element of a CAP <info><parameter> block (complex element) with a <valueName> of “EAS-STN-ID.”
  - Translation to EAS Station ID must pad the <value> element with the space character to 8 full bytes.
  - The Station ID SHOULD adhere to the character set limitations as defined in FCC Part 11.31(b), for example, the dash “-” and plus “+” characters are not permitted. Dash characters SHALL be converted to a slash '/', and plus characters SHALL be converted to a space.
- Messages for which the Governor’s “must carry” authority is invoked SHALL be marked by the inclusion of an additional CAP <info><parameter> block with a <valueName> of “EAS-Must-Carry” and a <value> of “True.” Such messages will be given appropriate priority in accordance with FCC regulations.

B.6.1 Constructing EAS Audio from IPAWS CAP v1.1 Profile

An EAS Audio message will be constructed as follows:

1. If attached audio with a CAP <resourceDesc> element <value> of “EAS Audio” is present, the EAS device SHALL use that attached EAS recorded audio as the audio portion of the EAS alert.

2. If attached EAS Audio is not present, and the EAS device supports text-to-speech technology, then text-to-speech audio SHALL be rendered as described in the “Constructing Text-to-Speech Audio from IPAWS CAP v1.1 Profile” section below and used as the audio portion of the EAS alert.

3. If none of the CAP elements required to construct a text-to-speech audio message as outlined in Figure 6 are present, then the expansion of the generated EAS message SHALL be used as the text, and rendered as text-to-speech.

4. If there is no attached EAS Audio, and the device does not support text-to-speech, the alert SHALL be sent as EAS-codes-only with no audio.

5. If an EAS Audio Uniform Resource Locator (URL) can not be accessed in a reasonable amount of time, then text-to-speech audio SHALL be rendered as described in the “Constructing Text-to-Speech Audio from IPAWS CAP v1.1 Profile” section below and used as the audio portion of the EAS alert. If the device does not support text-to-speech, the alert SHALL be sent as EAS-codes-only with no audio. The individual device user will decide what value to enter into the reasonable-amount-of-time value in that particular device.

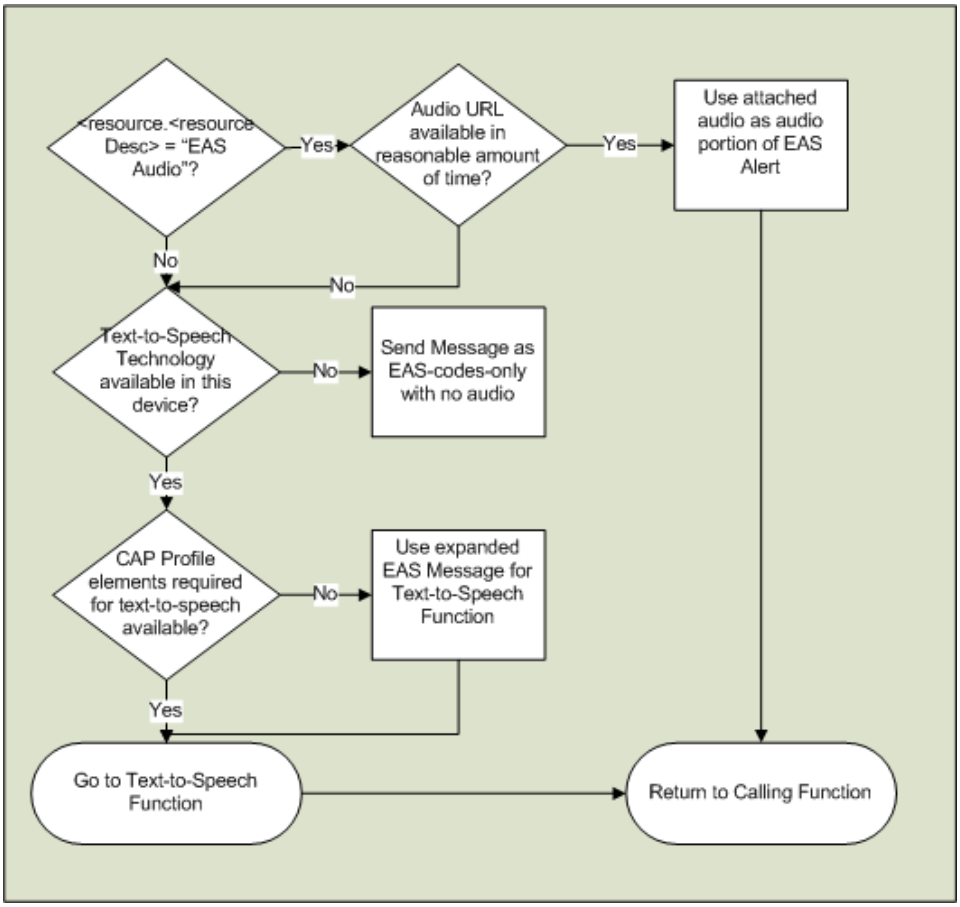


Figure 6 - Audio EAS Processing

B.6.2 Constructing EAS Recorded Audio from IPAWS CAP v1.1 Profile

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

- The audio SHALL be encoded as either an MP3 file as mono, 64 kbit/s data, preferably sampled at 22.05 kHz or otherwise at 44.1 kHz, or as a WAV PCM file as mono, 16-bit, sampled at 22.05 kHz.
- The CAP <resourceDesc> element <value> SHALL be "EAS Audio".
- The audio SHOULD be a reading of the same text as that in the CAP elements described below, so that the recorded audio message will match the video display message:
    - A sentence containing the Originator, Event, Location and the valid time period of the EAS message as represented in the EAS ZCZC Header Code as required in FCC Rules Part 11.51(d), followed by,
    - The words "This is the" followed by the full text of, or at least the first ten words from, the CAP <senderName> element, or if a <senderName> is not used by the words "Emergency Alert System", followed by,

- The full text of, or at least the first ten words from, the CAP <headline> element, followed by,
- The full text of, or at least the first ten words from, the CAP <event> element, followed by,
- The full text of, or at least the first one hundred words from, the CAP <areaDesc> element, followed by,
- The full text of, or at least the first one hundred words from, the CAP <description> element; followed by,
- The full text of, or at least the first one hundred words from, the CAP <instruction> element.
- Whenever the text included from the CAP <headline>, <areaDesc>, <description> or <instruction> elements is shorter than the full original text, any deletion SHALL be indicated by a one-second pause immediately following the shortened section of text.

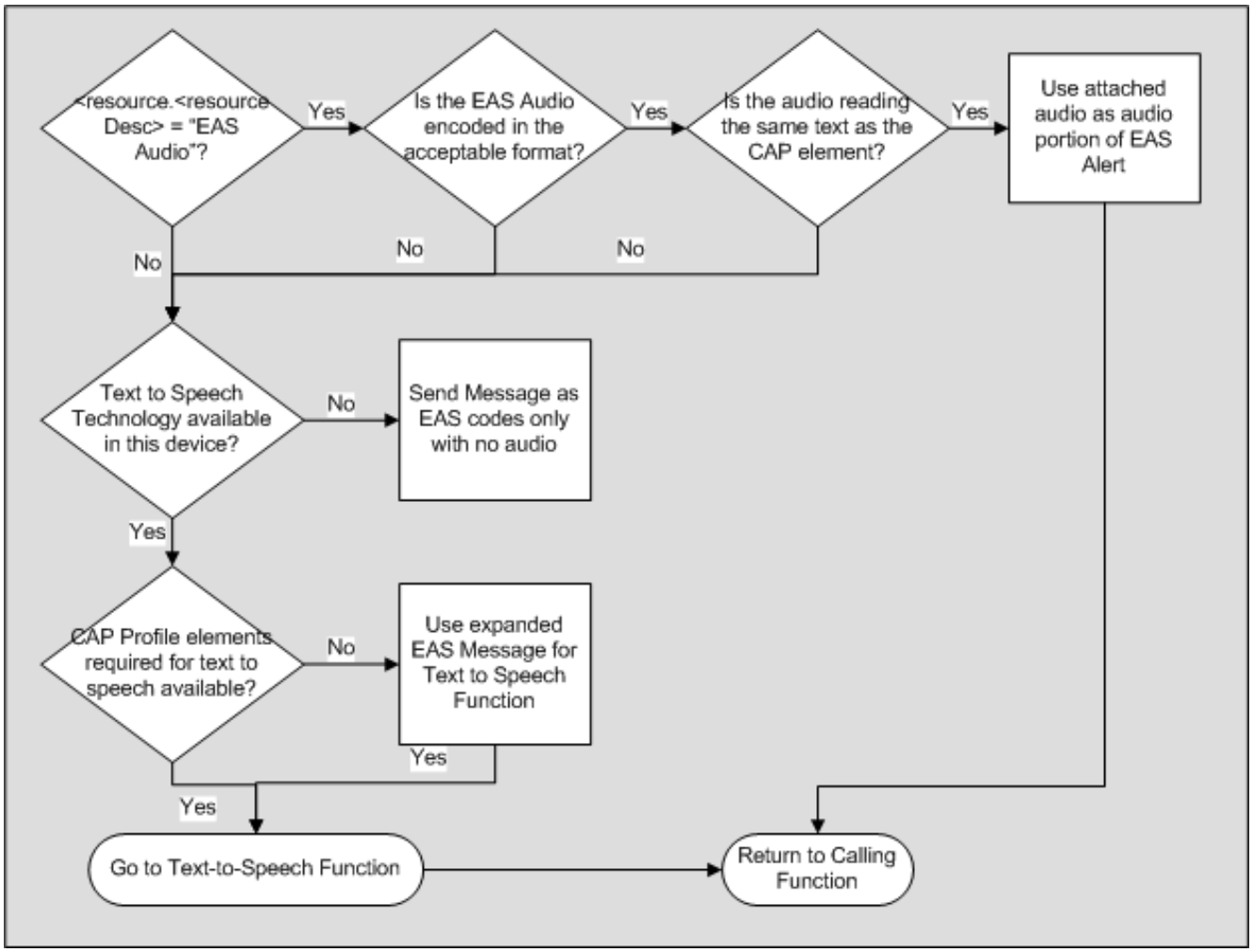


Figure 7: EAS Recorded Audio Processing

In the section above, the calculation for the maximum number of words in two minutes is based on 120 WPM. However, the FCC Part 11 two-minute limit on EAS messages will be enforced regardless of the speed used or the number of words.

There SHALL be an absolute maximum of the first 200 words recorded resulting from the combination of all of the above elements.

B.6.3 Constructing EAS Streaming Audio from IPAWS CAP v1.1 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:

- The CAP <resourceDesc> element value SHALL be “EAS Streaming Audio.”
- The audio SHALL use one of the following streaming methods:
  - MP3 streaming as either HTTP progressive-download streaming, or
  - MP3 streaming from a streaming server such as a Shoutcast™/Icecast™-compatible streaming server.

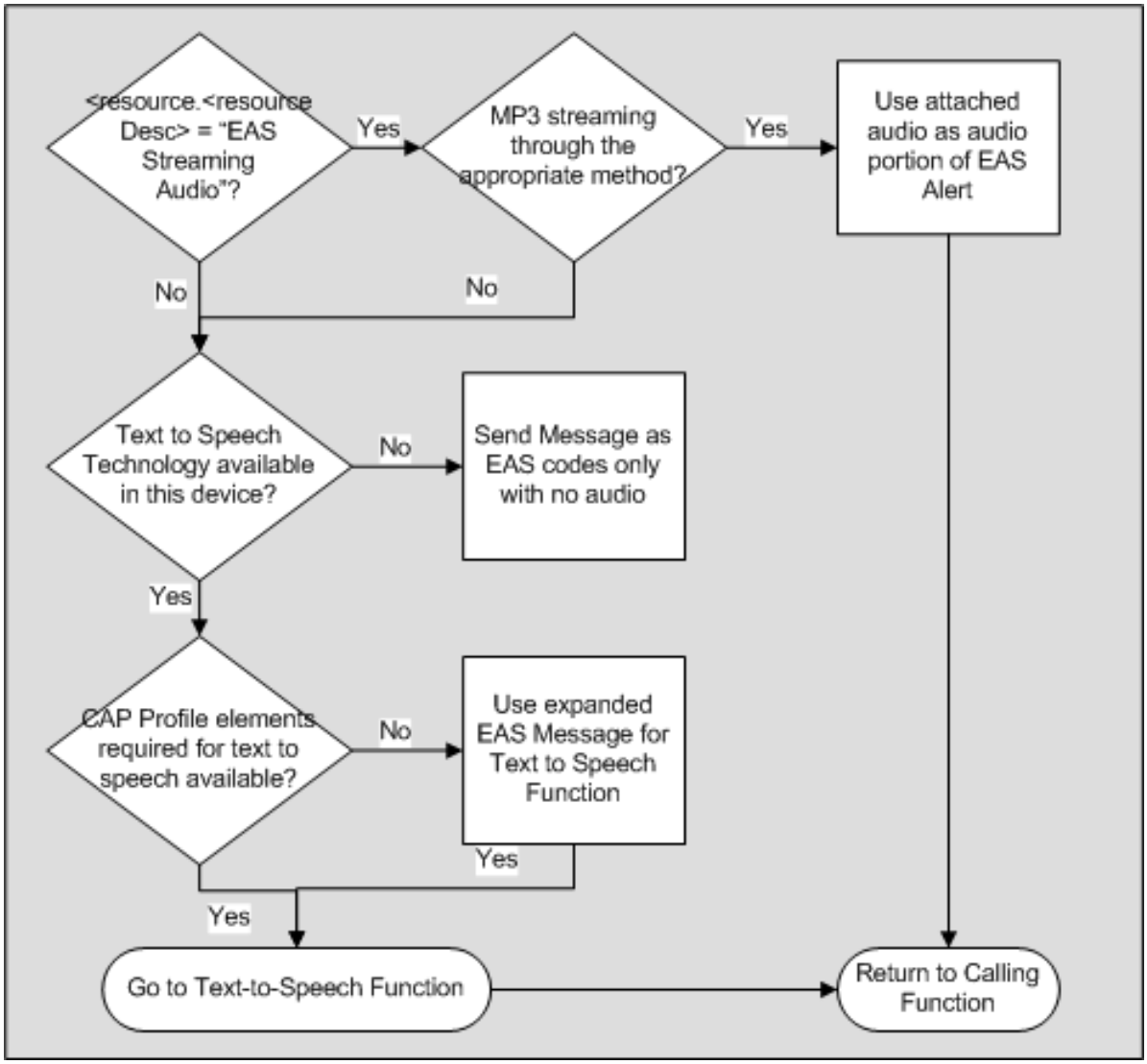


Figure 8: Streaming Audio EAS Processing

B.6.4 Constructing Text-to-Speech from IPAWS CAP v1.1 Profile

Where the CAP message is to be converted to audio using text-to-speech technology the delivered message SHALL consist of, and in the following order:

- A sentence containing the Originator, Event, Location, and the valid time period of the EAS message constructed from the EAS ZCZC Header Code as required in FCC Rules Part 11.51(d), followed by,
- The words “This is the” followed by the full text of, or at least the first ten words from, the CAP <senderName> element, or if a <senderName> is not provided by the words “Emergency Alert System”, followed by,
- The full text of, or at least the first ten words from, the CAP <headline> element, followed by,
- The full text of, or at least the first ten words from, the CAP <event> element, followed by,
- The full text of, or at least the first one hundred words from, the CAP <areaDesc> element, followed by,
- The full text of, or at least the first one hundred words from, the CAP <description> element; followed by,
- The full text of, or at least the first one hundred words from, the CAP <instruction> element.
- Whenever the text included from the CAP <senderName>, <headline>, <event>, <areaDesc>, <description> or <instruction> elements is shorter than the full original text, any deletion SHALL be indicated by a one-second pause immediately following the shortened section of text.

In the section above, the calculation for the maximum number of words in two minutes is based on 120 WPM. However, the FCC Part 11 two-minute limit on EAS messages will be enforced regardless of the speed used or the number of words.

There SHALL be an absolute maximum of the first 200 words rendered from the combination of all of the above elements.

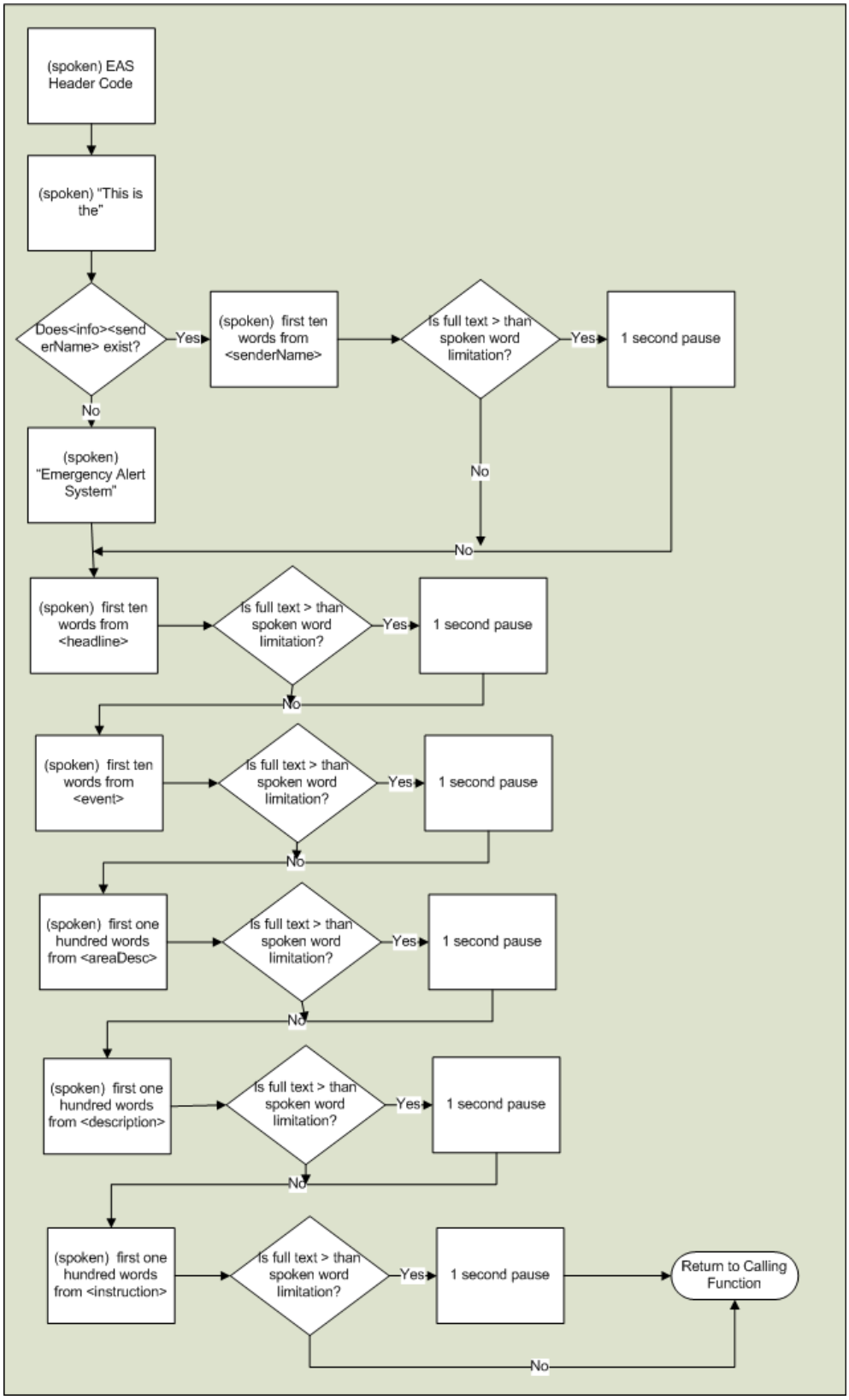


Figure 9 - Text to Speech EAS Processing

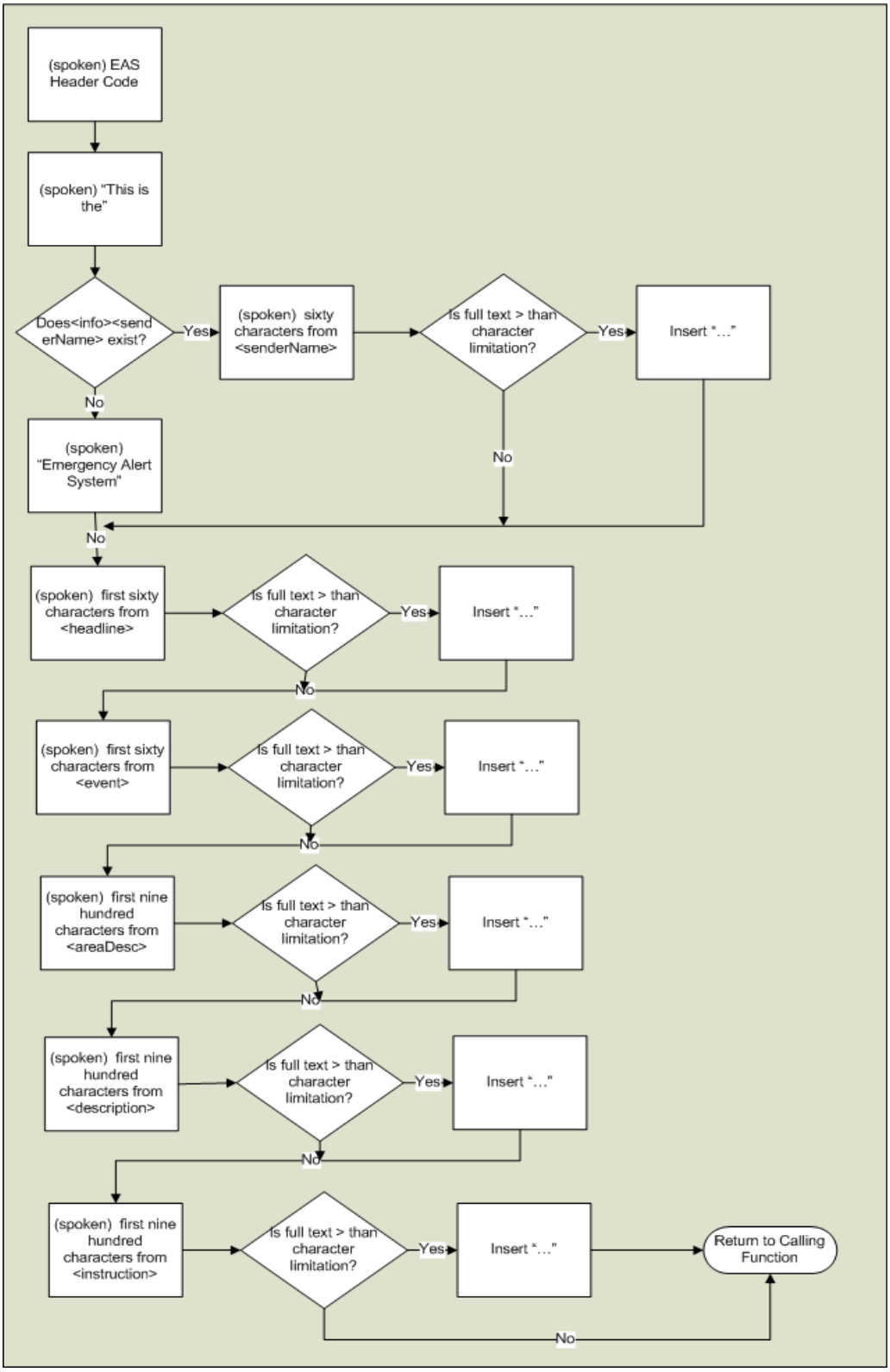
B.6.5 Constructing Video Display Text from IPAWS CAP v1.1 Profile

Where the CAP message is to be converted to text on a video display the delivered message SHALL consist of, and in the following order:

- A sentence containing the Originator, Event, Location and the valid time period of the EAS message constructed from the EAS ZCZC Header Code as required in FCC Rules Part 11.51(d), followed by,
- The words “This is the” followed by the full text of, or at least the first 60 characters from, the CAP <senderName> element, or if a <senderName> is not provided by the words “Emergency Alert System”, followed by,
- The full text of, or at least the first 60 characters from, the CAP <headline> element, followed by,
- The full text of, or at least the first 60 characters from, the CAP <event> element, followed by,
- The full text of, or at least the 900 characters from, the CAP <areaDesc> element, followed by,
- The full text of, or at least the first 900 characters from, the CAP <description> element; followed by,
- The full text of, or at least the first 900 characters from, the CAP <instruction> element.

Whenever the text included from the CAP <senderName>, <headline>, <event>, <areaDesc>, <description> or <instruction> elements is shorter than the full original text, any deletion SHALL be indicated by an ellipsis (“…”) immediately following the shortened section of text.

There SHALL be an absolute maximum of the first 1800 characters rendered from the combination of all of the above elements.



223

224 *Figure 10 - Video Display Text EAS Processing*

225 ## B.6.6 Appendix A. Acronyms

ASCII	American Standard Code for Information Interchange
ATIS	Alliance for Telecommunications Industry Solutions
CA	Class A television
CAP	Common Alert Protocol
CAPCP	Common Alerting Protocol Canadian Profile
CDC	Center for Disease Control
CFR	Code of Federal Regulations
CIV	Civil authorities
CMAS	Commercial Mobile Alerting System
DAB	Digital Audio Broadcast
DBS	Direct Broadcast Satellite
DE	Distribution Element
DHS	Department of Homeland Security
DOM	Document Object Model
EAS	Emergency Alert System
EAS-STN-ID	EAS Station Identification
ECIG	EAS-CAP Industry Group
EDXL	Emergency Data Exchange Language
EDXL-CAP	Emergency Data Exchange Language Common Alert Protocol
EDXL-DE	Emergency Data Exchange Language Distribution Element
EEE	EAS Event code Element
EOC	Emergency Operations Center
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
HazCollect	HazCollect Non-weather Emergency Messages
IPAWS	Integrated Public Alert and Warning System
ISO	International Organization for Standardization
ITFS	Instructional Television Fixed Service

LPFM	Low Power FM
LPTV	Low Power TV
MDS	Multipoint Distribution Service
MMDS	Multichannel Multipoint Distribution Service
NOAA	National Oceanic and Atmospheric Administration
OASIS	Organization for the Advancement of Structured Information Standards
OIC	Office for Interoperability and Compatibility
ORG	Originator Code
PEP	Primary Entry Point
PMO	Project Management Office
RFC	Request for Comments
SDARS	Satellite Digital Audio Radio System
TIA	Telecommunications Industry Association
URL	Uniform Resource Locator
WPM	Words Per Minute
WXR	National Weather Service
XML	Extensible Markup Language

226
227

C. CAP v1.1 IPAWS Exchange Partner System Requirements – Non-Normative

The following table specifies the REQUIRED constraints placed by the CAP v1.1 IPAWS Profile Exchange Partner Alert Systems on a CAP v1.1 message in order for the message to be processed by the EAS, the CMAS and the NOAA NWS HazCollect System. This table contains only those elements of CAP v1.1 for which there is IPAWS Exchange Partner Alerting System-specific annotation of interest. CAP v1.1 elements not included here simply means there is no specific constraint or condition in the use of those elements for any of these IPAWS Exchange Partner Alert Systems..

Appendix C Table: CAP v1.1 IPAWS Profile Exchange Partner System-specific Requirements (Non-Normative)

CAP Element	EAS	CMAS	Hazcollect NWEM
	(EAS-CAP Industry Group Recommendation 9/23/08)	(CMAS Architecture and Requirements, CMSAAC 2007)	(Instructions for Using the NOAA HazCollect Interface, v 0.3, 6 Nov 2008)
identifier			(1) Must be unique throughout HazCollect universe
sent	(1) Time zone mandatory.	(1) Time zone mandatory. Note: CMAS C-Interface requires UTC plus offset and must be consistent with any associated update or cancel messages	
status	(1) Must be "Actual" to be aired even for EAS test messages	(1) "Draft" will be rejected by CMAS Federal Alert gateway.	
msgType		(1) "Ack" will be rejected by CMAS Federal Alert Gateway.	
source			(1) Sender signature (name/initials).
scope		(1) Any value but "Public" will be rejected by CMAS Federal Alert Gateway.	(1) Must be "Public" or system will reject.

234

CAP Element	EAS	CMAS	Hazcollect NWEM
restriction		(1) If present CMAS Federal Alert Gateway will reject message.	
addresses		(1) If present CMAS Federal Alert Gateway will reject message.	
note	(1) If msgType is "Ack", should include "Ignored:", "Accepted:" or "Aired on:" plus station callsign		
info *			(1) Only one permitted.
language		(1) English only	(1) REQUIRED: May only be en-US or sp-US.
event			(1) REQUIRED. String must match NWEM name for corresponding eventCode
responseType *		(1) Value of "Assess" will result in rejection by CMAS Federal Alert Gateway. (2) Additional value of "Avoid" recommended.	
urgency	(1) Should be "Unknown" if the eventCode is DMO, NMN, NPT, RMT and RWT.	(1) Only messages with urgency of "Immediate" and "Expected" will be passed to the CMSPs	
severity	(1) Should be "Minor" if the eventCode is DMO, NMN, NPT, RMT and RWT.	(1) Only message with a severity of "Extreme" or "Severe" will the passed to CMSPs	

235

CAP Element	EAS	CMAS	Hazcollect NWEM
certainty	(1) Should be "Unknown" if the eventCode is DMO, NMN, NPT, RMT and RWT.	(1) Only message with a certainty of "Observed" or "Likely" will the passed to CMSPs	
eventCode*	(1) REQUIRED. The valueName must be "SAME", the value must be SAME three-letter event code.	(1) If value is "EAN" CMAS Federal Alert Gateway will process as Presidential. (2) If value is "CAE" CMAS Federal Alert Gateway will process as Child Abduction. (3) CMAS Federal Alert Gateway will ignore messages marked "NIC" or "EAT". (4) The CMAS specifications recommends that an eventCode also be present to assist in the generation of the alert text.	(1) REQUIRED: The valueName must be "SAME", the value must be SAME three-letter event code.
expires	(1) REQUIRED: Time zone mandatory.	(1) If already expired CMAS Federal Alert Gateway will reject. (2) If expires is missing, the Federal Alert Gateway will calculate a default expiration date and time. (3) UTC plus offset is mandatory. (1) Note: the CMAS C-Interface limits alerts to a maximum of 24 hours	(1) REQUIRED: Must conform to EAS expiration intervals (15 minute increments up to 120 minutes, 30 minute intervals up to 360, 360 max.)
senderName			(1) REQUIRED: String must match DMIS COG id used for login.

236

CAP Element	EAS	CMAS	Hazcollect NWEM
parameter *	(1) Two REQUIRED for EAS transmission: (2) First valueName of "EAS-ORG" with value of SAME ORG code: (3) Second valueName of "EAS-STN-ID" with SAME station ID: (4) Third OPTIONAL with valueName of "EAS-Must-Carry": and, (5) value of "TRUE" for gubernatorial alerts.	(1) OPTIONAL parameter with valueName of "CMAMtext" provides free text as alternative to the automatically constructed CMAS message. (2) There is a 90 English character limit in the free form text. (3) Any free form text must comply with the FCC rules & CMSAAC recommendations.	
resourceDesc	(1) If <resource> is used, value must be "EAS Audio" or "EAS Streaming Audio" as appropriate.	(1) Initial version the CMAS C-Interface is text only. (2) Multimedia formats such as audio and video are not pushed to the CMSPs on the C-Interface.	
mimeType	(1) Recorded audio must be MP3 64kbps 22.05 or 44.1 kHz samping, or WAV PCM, mono, 16-bit, 22.05 kHz sampling. (2) Streaming audio must be MP3 via HTTP or Shoutcast/Icecast service.		

CAP Element	EAS	CMAS	Hazcollect NWEM
area *	(1) Only the first <area> block will be processed.		
geocode *	(1) REQUIRED: valueName of "SAME" and value of 6-digit location code (extended FIPS).	(1) CMAS specification currently uses a 5-digit FIPS code as well as codes for states and regions.	(1) REQUIRED: May have valueName of "fips" with 5-digit FIPS code, or "state" with two-letter state code, or "zone" with NOAA zone designator.

*May have multiple occurrences in a message under CAP 1.1 spec

D. Acknowledgements

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

Aviv Siegel, AtHoc, Inc.
Art Botterell, Conta Costa County Community Warning System
Tim Grapes, Evoluntion Technologies, Inc.
Lee Tincher, Evolution Technologies, Inc.
Rex Brooks, Individual Member
Gary Ham, Inidividual Member
Jacob Westfall, Individual Member
Thomas Ferrentino, Individual Member
Robert Bunge, NOAA's National Weather Service
Sukumar Dwarkanath, SRA International
William Kalin, U.S. Department of Homeland Security
Richard Vandame, U.S. Department of Homeland Security
Patrick Gannon, Warning Systems, Inc.
Elysa Jones, Warning Systems, Inc.

E. Revision History

Revision	Date	Editor	Changes Made
‘WD.01	1-26-2009	Rex Brooks	First Draft.
WD.02	1-27-2009	Rex Brooks	Updated Table of Contents; Added Text to Section 1.1; Added Revision History
WD.03	1-29/2009	Rex Brooks	Full Subcommittee Revision of Section 1,
WD.04	2-3-2009	Rex Brooks	Multiple updates per CAP Profiles Subcommittee decisions.
WD.041	2-5-209	Rex Brooks	Multiple updates per CAP Profiles Subcommittee decisions.
WD.042	2-10-2009	Rex Brooks	Move Sections 3 to an Appendix; Insert FEMA CAPv1.1 Profile Requirements v2.4 Public as Appendix; Delete Section 4; Prepare Document for vote to submit to Emergency Management Technical Committee per CAP Profiles Subcommittee decisions.
WD.05	2-12-2009	Rex Brooks	Final prep for report out to the TC.