

Federal Emergency Management Agency (FEMA)



FEMA

Integrated Public Alert and Warning System – Open Platform for Emergency Networks (IPAWS-OPEN) Common Alerting Protocol Message Construction Guide

**Version 0.4
April 8, 2011**

Document Revision History

Document Location

Location
File Path:

Revision History

Version Number	Version Date	Summary of Changes	Team/Author
0.1	12/25/2010	Initial Creation of Document	Gary Ham
0.2	12/29/2010	Review / edit	Neil Graves
0.3	1/25/2011	Draft complete with some embedded questions. Potential AMBER requirements are TBD.	Gary Ham
0.4	4/8/2011	Edits from Neil Bourgeois, Kirby Rice, and Amy Sebring. Restructure and other edits from Mark Lucero	Gary Ham
0.5	4/18/2011	Typographical editing from Amy Sebring	Gary Ham

Table of Contents

Document Revision History	2
Document Location	2
Revision History	2
1 Introduction	5
1.1 Purpose.....	5
1.2 Scope.....	5
1.3 References.....	5
2 Before You Begin	6
3 IPAWS, IPAWS-OPEN, and CAP	7
3.1 Mission, Vision, and Goals.....	7
3.2 Architecture.....	7
3.3 CAP as the Organizing Driver of IPAWS Message Distribution.....	8
4 IPAWS Process Flow Summary	9
4.1 Processing CAP Input.....	9
4.2 Determining IPAWS Channel Dissemination	11
5 SOAP Validation	14
6 CAP Validation Requirements	14
6.1 CAP Schema Validation	14
6.2 CAP Header Data Restrictions and Suggestions	14
6.3 CAP INFO Block Data Restrictions and Suggestions	17
6.4 CAP Resource Block Data Restrictions and Suggestions.....	21
6.5 CAP Area Block Data Restrictions and Suggestions.....	23
6.6 CAP Message Level Digital Signatures.....	24
6.7 Using IPAWS-OPEN for Basic CAP Exchange.....	25
7 IPAWS Profile Validation and Processing	26
7.1 IPAWS Profile Validation Requirements	26
7.2 IPAWS-OPEN Processing of IPAWS Profile Identified Messages	30
8 IPAWS Dissemination Channel Processing	31
8.1 Digital Signatures (again)	31
8.2 EAS Requirements.....	31
8.2.1 EAS Data Restrictions and Suggestions	31
8.2.2 EAS Message Construction	34
8.2.3 EAS Message Distribution Channels.....	35
8.3 NWEM Requirements.....	35
8.3.1 NWEM Data Restrictions and Suggestions	35

8.3.2	NWEM Authorization and Training Requirements (Developer’s Viewpoint)	39
8.3.3	NWEM Message Distribution Channels	39
8.4	CMAS Requirements	39
8.4.1	CMAS Data Restrictions and Suggestions	39
8.4.2	CMAS Message construction	40
8.5	Amber Alert Requirements	41
9	Access to IPAWS-OPEN messages	42
9.1	CAP Query Metadata in IPAWS-OPEN	42
9.2	Data Access Questions	42
9.3	Data Content and Usage Queries	43
9.3.1	Basic CAP Elements used as Retrieval Metadata	43
9.3.2	Geographic Elements used as Retrieval Metadata	43
9.3.3	Dissemination Path Retrieval Metadata	43
10	Summary and Suggested Course for Development of a CAP Interface	44
11	Appendix A - Event Code Applicability by Dissemination Channel	45
12	Appendix B - Acronyms	48

1 Introduction

The Integrated Public Alert and Warning System - Open Platform for Emergency Networks (IPAWS-OPEN) provides interoperability interfaces for sharing of alerts, situation reports, common operational picture snapshots, and other emergency related information. It also acts as the primary aggregator for IPAWS Public Alerts to be originated by authorized warning officials and disseminated via internet, Cellular Broadcast, NOAA Radio broadcast, and Emergency Alert Service (EAS) Broadcast.

1.1 Purpose

This document is designed to help developers and system designers build Common Alerting Protocol (CAP) Messages for all purposes appropriate to the IPAWS aggregator. This is primarily a technical “how-to” document, but includes the functional purpose for each technical item to be discussed.

1.2 Scope

This document will introduce and address content requirement details for CAP Version 1.2 messages posted to the IPAWS-OPEN postCAP Aggregator interface for all modes of distribution defined for IPAWS to include:

- Private and/or Restricted – Retrieval Only
- Public – Retrieval Only
- Public - RSS Feed
- Public EAS – Private RSS Feed
- Public NWEM – NOAA Radio Broadcast
- Public CMAS – Cell phone Broadcast

1.3 References

The following documents were used to obtain source information or are referenced in this document:

- Federal Emergency Management Agency (FEMA), Integrated Public Alert and Warning System (IPAWS) Open Platform for Emergency Networks (IPAWS-OPEN v2) Web-Service Interface Design Guidance Version 1.2, November 12, 2010
- OASIS Common Alerting Protocol, Version 1.2, OASIS Standard, 01 July 2010
- IPAWS Authorized Originator Permission Procedures for IPAWS COGs (to be published)
- National Weather Service Instruction 10-1701, Text Product Formats and Codes, February 12, 2003
- Common Alerting Protocol, v.1.2 USA Integrated Public Alert and Warning System Profile Version 1.0, Committee Specification 01, 13 October 2009
- ECIG Recommendations for a CAP EAS Implementation Guide, EAS CAP Industry Group – ECIG, EAS-CAP Implementation Guide SubCommittee, Version 1.0, 17 May 2010

- Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification, October 2009

2 Before You Begin

A Memorandum of Agreement for test and Development with IPAWS is required. Please visit <http://www.fema.gov/emergency/ipaws/aggregator.shtm> for information about OPEN Web-Services. While this document will help, on its own, with an understanding of the various CAP options, you will not be able to test implementation in your solutions until you have first established a connection to IPAWS. That connection is outside the scope of this document, which is purely focused on CAP content requirements.

3 IPAWS, IPAWS-OPEN, and CAP

3.1 Mission, Vision, and Goals

IPAWS Vision: Timely Alert and Warning to American People in the preservation of life and property.

IPAWS Mission: Provide integrated services and capabilities to local, state, and federal authorities that enable them to alert and warn their respective communities via multiple communications methods.

IPAWS Goals: Create and maintain an integrated interoperable environment for alert and warning; make alert and warning more effective; and strengthen the resilience of the IPAWS infrastructure.

3.2 Architecture

IPAWS-OPEN (in its message aggregator role) is a FEMA operated message broker that provides authentication and non-repudiation to messages posted from alerting authorities. It then either pushes appropriate messages to appropriate dissemination pathways, or allows retrieval (through polling) of messages from authorized users.

Figure 3-1 is an Operational View of IPAWS showing IPAWS-OPEN in its role as the National Alert aggregator for IPAWS. On the left side of the drawing, Alerting Authorities (Alert Originators) at all levels are shown as able to exchange alerts with each other directly or using IPAWS-OPEN as a message broker between systems. The right side shows dissemination channels for public alerts to include the Emergency Alert System, Commercial Mobile Services (cell phones), public internet access, NOAA Radio Broadcast, and a variety of customized services that can be created for specialized alert and warning. Both the left and the right sides of the drawing, while part of the IPAWS Architectural vision, are not directly controlled by IPAWS. Instead they are implemented by private industry and by government authorities at all levels of government to meet their individual needs.

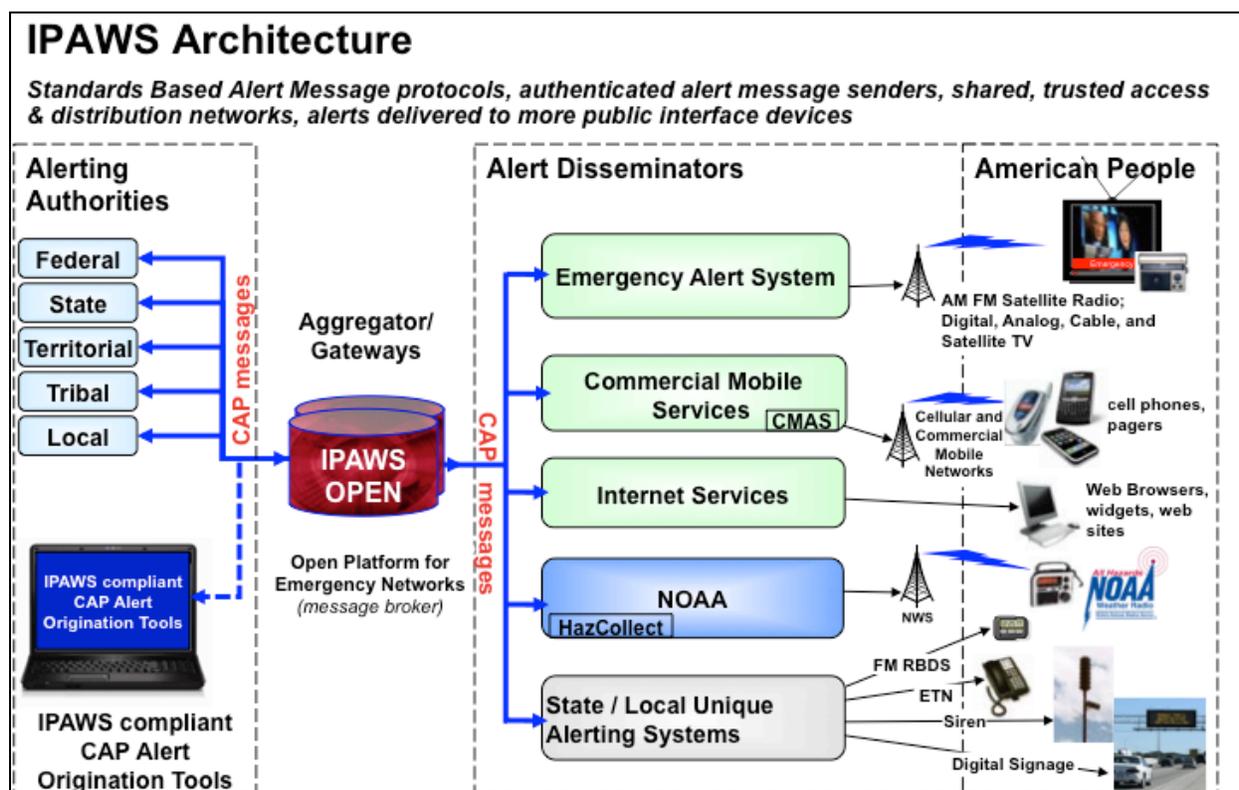


Figure 3-1: IPAWS-OPEN Architecture

3.3 CAP as the Organizing Driver of IPAWS Message Distribution.

CAP is a messaging data standard that facilitates interoperability with the IPAWS-OPEN alert aggregator. All posted alerts must validate to CAP, allowing the aggregator to further inspect the contents of the message for data determines the actual distribution path(s) for the message. Based on the data, an originator can:

1. Create a non-IPAWS CAP message that is sent only to specific addresses (COGs) in IPAWS. This message can be:
 - a. Private – Intended only for the recipient,
 - b. Restricted – Allowing the recipient to know the rules for redistribution, or
 - c. Public – Giving the recipient full latitude in redistribution.
2. Create an IPAWS Profile conformant CAP message that will be available to the general public via RSS Feed. The IPAWS Profile message can also be distributed via:
 - a. Emergency Alert System (EAS) Broadcast,
 - b. NOAA Radio as a Non-weather Emergency Message (NWEM), and/or
 - c. Cell phone via the Cellular Mobile Alert System (CMAS).

The remainder of this document will be focused on the specific data found in an incoming CAP message that drives its distribution and the process by which that data is evaluated.

4 IPAWS Process Flow Summary

When processing a CAP 1.2 message posted to the IPAWS postCAP functionality, the IPAWS system asks a series of eight questions, all of which can be answered by the content of the posted message as specified in the sections 5 through 8 below. The first four questions are geared to determining whether to accept the message and store it for retrieval by authorized IPAWS-OPEN participant systems. The second four questions are designed to determine which, if any, IPAWS dissemination channels will be used to actually push messages to the general public.

4.1 Processing CAP Input

Figure 4-1 illustrates the logic and flow of IPAWS-OPEN processing of a Posted CAP message. Unless formal validation errors are found, all CAP messages sent to the IPAWS postCAP interface are saved for retrieval by Authorized IPAWS-OPEN participant systems. Those messages that qualify are also processed for IPAWS push dissemination (sections 7 and 8 below).

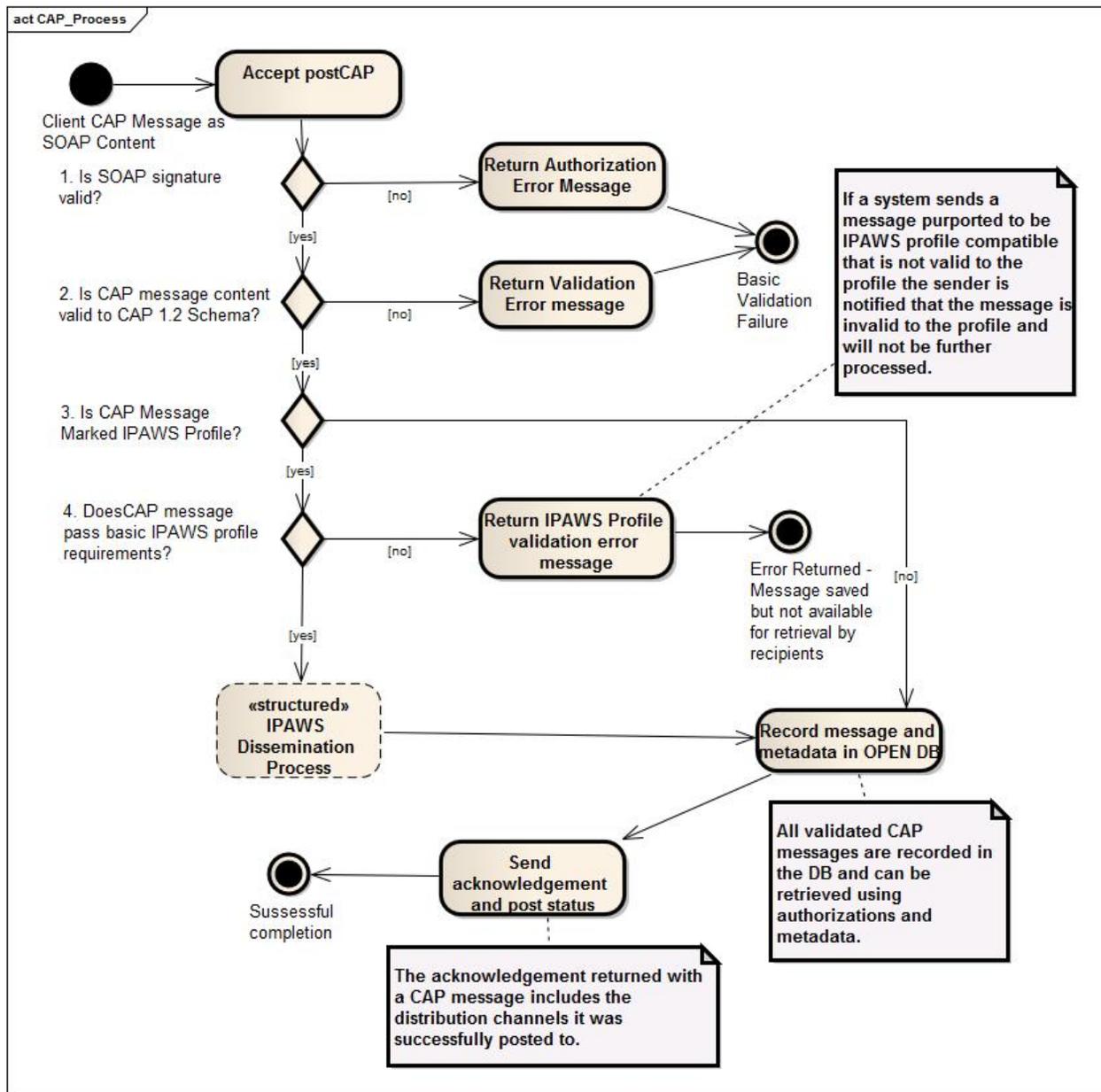


Figure 4-1 IPAWS-OPEN CAP Message Processing

1. Is the SOAP signature valid? Posters must wrap their CAP messages in a SOAP envelope as described in the IPAWS programmers Guidance document. That SOAP envelope must implement WS-Security with a FEMA supplied x509 certificate that is assigned to an operational IPAWS COG. If that signature fails or the SOAP Envelope is malformed, the message is rejected and an error message is returned. (See section 5 below.)
2. Is the contained CAP message valid with respect to the CAP 1.2 Schema? All message posted to the CAP 1.2 postCAP interface will be subjected to content validation against

the formal CAP 1.2 schema. Messages that fail will be rejected and an error message indicating the reason will be returned. (See section 6 below.)

3. Is the valid CAP 1.2 message marked as an IPAWS Profile conformant message? If a message is not marked as a formal IPAWS message using the <code> element, it will be stored to the IPAWS-OPEN database and be retrievable based on the data in the message as defined in section 9 below. It will not be forwarded to IPAWS dissemination channels nor will it be forwarded to any IPAWS feed. It will only be available through retrieval by authorized IPAWS interoperable systems using authenticated retrieval connections. Section 9 provides retrieval rules and parameters.
4. Does the CAP 1.2 message pass basic IPAWS Profile Requirements? Section 7 below defines the basic prerequisites for all IPAWS Profile conformant messages. If a message is marked as an IPAWS profile message, but does not meet the requirements in the formal specification, it is an invalid message, even if it validates to the CAP 1.2 schema. Such messages will be treated by IPAWS-OPEN as invalid and will not be made available for retrieval, nor will they be pushed to any IPAWS dissemination channel. Messages that pass basic IPAWS profile validation will be saved in the database and made available for retrieval by authorized users. Push dissemination by IPAWS, however, is not automatic for all IPAWS Profile conformant messages. A validated signature is required.

4.2 Determining IPAWS Channel Dissemination

All messages that successfully pass questions one through four above are processed for IPAWS distribution channel dissemination. Figure 4.2 below is a breakout of the “IPAWS Dissemination Process” activity bubble in Figure 4.1 above. It shows four more questions (5 through 8) that determine which, if any, IPAWS channels are used by IPAWS-OPEN to distribute IPAWS Profile Conformant CAP messages received by IPAWS-OPEN.

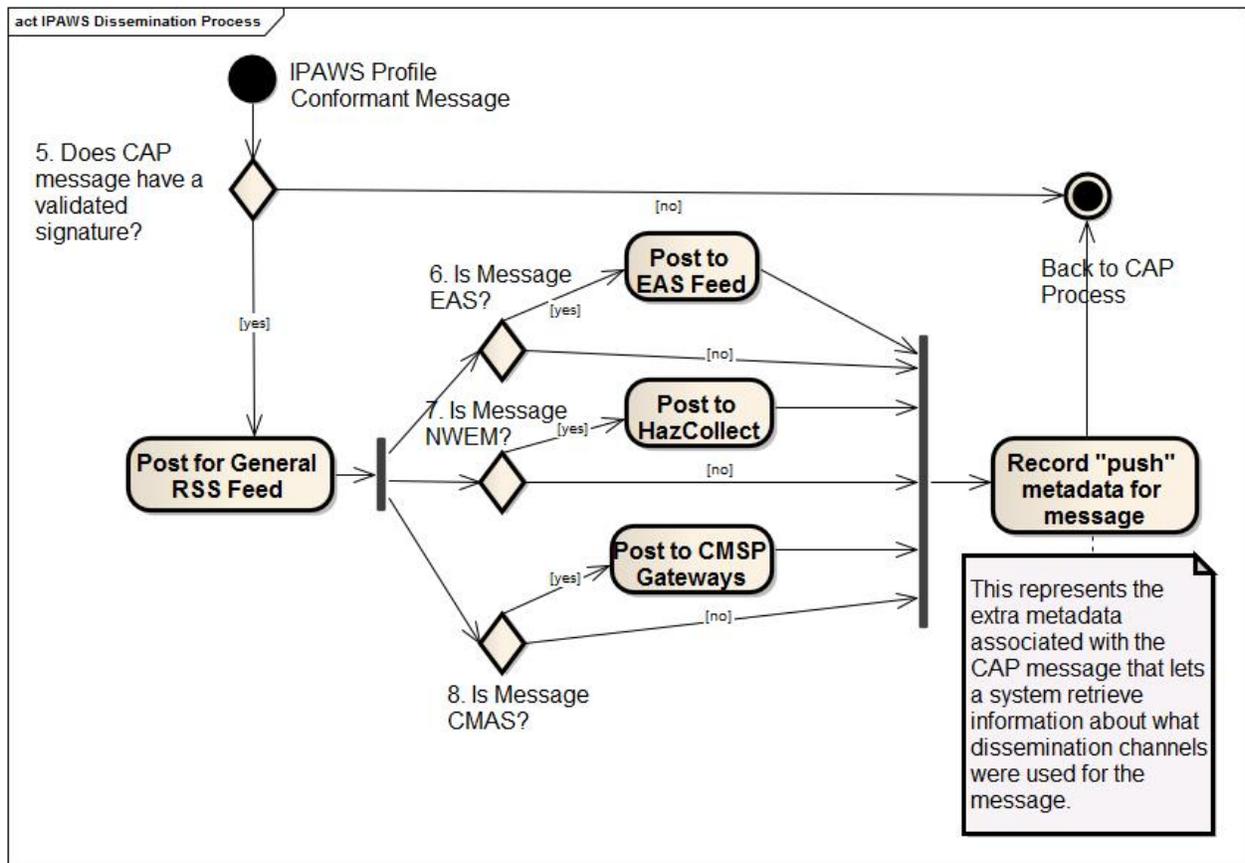


Figure 4-2 IPAWS Public Dissemination Processing

5. Does the IPAWS Profile Conformant CAP message include an IPAWS verified digital signature? (Section 8.1 below applies.) Before an IPAWS Profile conformant message can be pushed to channels that may be accessed by unknown users, there must be a mechanism to ensure the non-repudiation of the originating organization. So the final screening before IPAWS push dissemination methods are employed is for IPAWS-OPEN to verify that there is a digital signature in place on the message and that the digital signature is recognized as one that was issued through FEMA and approved for use by the message origination COG. If the message level signature screening is successful, the message is forwarded to the public RSS feed for public access. It is also processed for further dissemination to the private RSS feed for EAS Broadcasters, to NOAA Radio Broadcast, and/or to CMAS broadcast. Based upon its content, it may be sent to none of these added channels, one or more of them, or all of them, as appropriate. If the signature screening is not successful, the message is maintained by IPAWS-OPEN for authorized retrieval, but it is not pushed to formal IPAWS dissemination channels.
6. Is the IPAWS Profile Conformant CAP message with an IPAWS verified Digital Signature designed for EAS Broadcast? All messages that pass question 5 are considered for this question. In order to answer this question IPAWS-OPEN applies the criteria

found in Section 8.2 below. If all requirements are met, the message is made available and/or pushed to EAS broadcast gateways.

7. Is the IPAWS Profile Conformant CAP message with an IPAWS verified Digital Signature designed for NOAA Broadcast as a Non-Weather emergency Message? All messages that pass question 5 are independently considered for this question, regardless of whether they pass question 6 or not. In order to answer this question IPAWS-OPEN applies the criteria found in Section 8.3 below. If all requirements are met, the message is translated to NOAA's required format and posted to NOAA's Hazcollect server for NOAA Radio Broadcast.
8. Is the IPAWS Profile Conformant CAP message with an IPAWS verified Digital Signature designed for CMAS broadcast? All messages that pass question 5 are independently considered for this question, regardless of whether they pass questions 6 and/or 7. In order to answer this question IPAWS-OPEN applies the criteria found in Section 8.4 below. If all requirements are met, the message is translated to the format required by cellular providers to CMSP gateways as appropriate.

There is a ninth question that remains to be determined. That question concerns the processing of a Civil Abduction Emergency (aka Amber Alert). This capability will be introduced in a future release.

Once the dissemination channels are determined, their use is recorded for the message. This allows originators to retrieve information in the future about where their messages were actually sent. The process then returns to the final step in Figure 8.1 above which shows that all validated CAP messages (IPAWS Profile Conformant and regular CAP) are recorded by IPAWS for retrieval by authorized member systems in the IPAWS-OPEN network.

5 SOAP Validation

Posting to IPAWS-OPEN requires that the interoperating system send a SOAP message signed using WS-Security v1.0 to the designated IPAWS-OPEN web service. Instructions for how to accomplish this action are found in the IPAWS-OPEN programmers design guidance document:

- Federal Emergency Management Agency (FEMA), Integrated Public Alert and Warning System (IPAWS) Open Platform for Emergency Networks (IPAWS-OPEN v2) Web-Service Interface Design Guidance Version 1.2, November 12, 2010.

6 CAP Validation Requirements

This section provides requirements and suggestions that apply to all CAP messages bound for the IPAWS-OPEN message broker; whether they are IPAWS Profile conformant messages or just regular CAP messages.

6.1 CAP Schema Validation

Signed SOAP alert messages brokered by IPAWS-OPEN will have a single instance of a valid CAP 1.2 message as content in the SOAP envelope. The first thing that the IPAWS-OPEN Alert Aggregator will do after validating the signature in the SOAP envelope will be to validate the content is indeed a valid CAP 1.2 message. To do so, it will validate the contents against the XML schema found in the formal CAP Specification:

- OASIS Common Alerting Protocol, Version 1.2, OASIS Standard, 01 July 2010

If the message fails validation, it will be summarily rejected and an error message will be returned to the system attempting to post the message. There are several other restrictions in the CAP standards that may, or may not, be strictly enforced by IPAWS-OPEN and/or other CAP networks because these rules cannot be enforced by schema alone. These will be discussed by individual element in the following sections.

6.2 CAP Header Data Restrictions and Suggestions

The header portion of a CAP <alert> message contains elements used to identify, categorize, and route the contained warning information. The actual warning information is found in one or more <info> elements that are found in the alert following the header data.

1. Extended Identifier: In the CAP Standard, there is the notion of an extended unique identifier composed of the following explicit combination of elements: <sender>,<identifier>,<sent>. Many systems will use a unique <identifier> or a unique combination of <sender>, <identifier>. This is not wrong per the specification, but <references> must be built as a comma delimited triplet and, if multiple message references are needed in <references> they should be space delimited. That means, of course that there can be no spaces or commas within the <identifier>, <sender>, or

- <sent> contents of a CAP message (e.g. ,“George Smith” is an improperly formatted value for <sender>).
2. Message ID <identifier>: IPAWS-OPEN 2.0 enforces uniqueness by Collaborative Operations Group (COG) in the message that it accepts. In the future, IPAWS-OPEN may add global enforcement of uniqueness of the combination of <sender> and <identifier> to its current requirement of unique identifier for a COG. This element must not contain white space, commas, ‘<’, or ‘&’.
 3. Sender ID <sender>: The CAP specification requires that <sender> be a globally unique identifier for identifying a sender. The use of any Internet domain name based identifier for the sender could guarantee uniqueness (e.g. “com.domain.systemusername”, an email address, or the MAC address for a machine-generated alert). This element must not contain white space, commas, ‘<’, or ‘&’.
 4. Sent Date/Time <sent>: This time value should be the time at which the message is first posted from an originator. The format must be represented in the DateTime Data Type format (e.g., "2012-05-24T16:49:00-07:00" for 24 May 2012 at 16:49 PDT). As a result alert originators should either use system time of post or some sort of widget to create the sent field, not have the user type data into the sent field manually. (Note: system time of post requires “durations” to calculate other xsd:datetime fields in order to comply with EAS and NOAA rules. See sections 8.2 and 8.3 below)
 5. Message Status <status>: This required field must contain one (of many) specific values; please see CAP v1.2 standard for allowed values. Per spec, <status>”Exercise” suggests that exercise identifier be entered in note. (This suggestion is not enforced by IPAWS-OPEN.)
 6. Message Type <msgType>: This required field must contain one (of many) specific values; please see CAP v1.2 standard for allowed values. Per spec, <msgType>”Error” suggests that erroneous message be referenced in <references>. (This suggestion is not enforced by IPAWS-OPEN, but may be in the future. It is highly recommended.)
 7. Source <source>: This optional field is a useful way of identifying whether the source was from a person or specific device. (Not used in IPAWS-OPEN, but applicable for NWEM see Section 8.3 below))
 8. Scope <scope>: This required field must have a value of “Public,” “Private,” or “Restricted.” In IPAWS-OPEN, “Private” or “Restricted” CAP messages will be available for retrieval ONLY by polling from a COG that is specifically identified in the <addresses> element. Public CAP messages will also be available by polling from a COG. ALL messages intended for any push mechanism (RSS, EAS, CMAS, or NWS) must have <scope> = “Public.” “Private” or “Restricted” CAP messages will not be pushed from IPAWS-OPEN.
 9. Restriction <restriction>: This optional element is to be used if and only if <scope> “Restricted.” It is not enforced in IPAWS-OPEN.
 10. Addresses <addresses>: This element must be used in a message has <scope> = “Private.” It is optional if <scope> “Public” or <scope> “Restricted.” It means that these

are addresses are where the message is specifically intended to go, whether they are allowed to go other places or not. IPAWS-OPEN **requires** the use of the <addresses> element to indicate all COGs that are allowed to retrieve a CAP message. **If the addresses element is missing or contains no value that equates to a known IPAWS-OPEN COG identifier, the message cannot be retrieved from IPAWS-OPEN using polling techniques.** This use of <addresses> offers some interesting opportunities for developers:

- a. If you want to post an alert for retrieval by other systems or users on your own COG, you can post a private alert to your COG only.
 - b. If you want to post a Public alert for RSS, EAS, CMAS, MWS push distribution, but do not want other polling applications to get it, you can post a public alert to your COG only.
 - c. If you want to post a Public alert for RSS, EAS, CMAS, MWS push distribution, and only want certain other polling applications to get it, you can post a Public alert to your COG and the COGs represented by the polling applications you want to receive the message.
 - d. If you want an alert to be retrieved by a particular organization (for review perhaps), but allow that organization to re-publish the message as desired, you can post a Public alert to the COG ID of that organization without the IPAWS Profile Indicator. In this case there will be no push to RSS etc. (See <code> below for further explanation.)
 - e. If you want to send alert to one or more organizations with whom you have a sharing agreement, but do not want them to go out to the world, you can post the alert as restricted with requested restriction in the <restriction> element and the Organizations you want to get the alert identified with COG IDs in <addresses>.
 - f. There is also the spam option. Putting COG ID 0 into <addresses> allows all polling COGs to retrieve an alert. This option should be used only for messages of National interest. Abuse could result in removal of alerting authority from the alert originating COG.
11. Handling Code <code>: An optional element representing “any user-defined flag or special code to flag the alert message for special handling.” This element may contain zero, one, or multiple codes. IPAWS-OPEN does not require <code> to accept a CAP message for polled retrieval. To be pushed over IPAWS channels, however, messages must contain an IPAWS indicator as a <code> element value (see section 7.1 below). For developers this means that you can enable your application to allow users to exchange CAP messages via IPAWS-OPEN without any IPAWS push dissemination to the public by simply not using the IPAWS indicator in a <code> element.
12. Note <note>: An optional element “describing the purpose of significance of the alert message.” It is “primarily intended for use with <status> “Exercise” and <msgType> “Error”. IPAWS-OPEN does not enforce this definition or suggested use.

13. Reference IDs <references>: An optional element per the schema that references previous CAP messages. The element uses an extended identifier in the form sender,identifier,sent to reference previous CAP messages (usually, but not exclusively, for <msgType> “Cancel,” “Update,” or “Error”). IPAWS-OPEN does not currently validate the internal content structure of this entry beyond what is already enforced by the schema, but certain downstream processing for EAS, NWEM, and CMAS alerts requires proper structure for dissemination. The <references> element must be built as a comma delimited triplet and if multiple message references are needed in <references> they should be space delimited. This means there can be no spaces or commas within the identifier, sender, or sent contents of a CAP message.
14. Incident IDs <incidents>: This optional element that is used to collate multiple messages referring to different aspects of the same incident. IPAWS-OPEN does not currently validate the internal content structure of this entry beyond what is already enforced by the schema and does not use this element for processing.

6.3 CAP INFO Block Data Restrictions and Suggestions

It is the <info> elements in the CAP message that contain all actionable warning information in a CAP <alert>. There can be more than one <info> block in a single <alert>. This is usually done for one of three reasons:

- Alert using multiple languages.
- Alert a different geographic area about the same issue, but with a different call to action because of a difference in proximity to the actual incident location.
- Provide a time sequence for the <alert> using different values for <effective> and <expires> in different <info> blocks as it applies to different geographic areas.

In general, a single <info> element is preferred. It is easier to work with and minimizes the ambiguity that can be associated with multiple <headline>, <description>, and <instruction> elements. IPAWS-OPEN will, however, accept messages for exchange with multiple <info> elements as prescribed in the formal CAP standard. This, of course, means that general purpose <alert> consuming software must also be prepared to handle multiple <info> blocks

It is actually possible to send a CAP message without an <info> element. The formal specification prescribes <info> as a 0-to-many structure. Missing <info> elements are generally acceptable for alert messages with <msgType> equal to “Cancel,” “Ack,” or “Error” only. “Ack” and “Cancel” messages should have a properly completed <references> element identifying a previous message that is being acknowledged or cancelled. “Error” messages indicate a message rejected by a receiving party. They should use <references> to identify the message that they are rejecting and <note> to identify the reason for the rejection. Even though it is not enforced by the schema, alert messages with <msgType> equal to “Alert” or “Update” should always have at least one <info> element. At the basic CAP level, IPAWS-OPEN does not enforce these rules beyond what is already enforced by the schema (i.e., it accepts any message that passes schema validation). Several <info> related requirements are in play, however, for

IPAWS Profile messages destined for EAS, NWEM, and CMAS. Details are provided in sections below as appropriate.

The IPAWS-OPEN requirements/suggestions for <info> sub elements are as follows:

1. Language <language>: This is an optional element. If omitted the value is assumed to be “en-US” (United State English) as defined in RFC 3066. IPAWS-OPEN does not currently validate the internal content structure of this entry beyond what is already enforced by the schema. It does use this element for IPAWS push functions. This usage will be described in the sections below.
2. Event Category <category>: A required element enforced by schema. This element could become a future basis for alert authority permission definition, but is not used for that purpose at this time.
3. Event Type <event>: This is a required plain text element “denoting the type of the subject event of the alert message.” For general CAP there are no restrictions on this element. Restrictions defined for specialized use (NWEM and EAS) are described in following sections. This entry often corresponds to the Event Name corresponding to Event Code <eventCode> as listed in Appendix A.
4. Response Type <responseType>: This is an optional, zero-to-many element populated from a pre-defined set of enumerated values that is enforced by schema validation. This element has particular value when translating CAP to a short message dissemination capability as it may be used as a substitute (or quick header) for the instruction element.
5. Urgency <urgency>, Severity <severity>, and Certainty <certainty>: These are three required elements that “collectively distinguish less emphatic from more emphatic messages.” All are populated from pre-defined sets of enumerated values that are enforced by schema validation. For general CAP IPAWS-OPEN imposes no restrictions on this element. Restrictions defined for specialized use (NWEM, EAS, and CMAS) are described in following sections.
6. Audience <audience>: This element is composed of optional text that describes the intended audience of the alert in human readable form. IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema. It does, as with all optional elements, accurately maintain the value as submitted and pass that value on through push and/or retrieval as appropriate.
7. Event Code <eventCode>: This is an optional, 0-to-many, element that should generally be thought of as a code or codes related to the <event> element above. It is one of three elements in CAP that are defined as structures requiring an included <valueName> and corresponding <value> as the content. The <valueName> designates the domain of the <value> while the <value> is a known string from that domain. At the basic CAP level, IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema. This element is used directly, however, in IPAWS Profile messages for EAS, NWEM, and CMAS and will be validated by IPAWS-OPEN for push to those dissemination channels. Details are provided in sections below as appropriate.

8. Effective Date/Time <effective>: This is an optional DateTime element that sets a specific begin time for the information contained in the <info> element. Where this element is not used, <sent> is assumed to be the effective time of the warning. Generally there is no reason to use this element unless there are multiple <info> elements in the message, each with a different desired time to go into effect. At the basic CAP level, IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema. (For example, IPAWS-OPEN does not do time calculations on <effective> to determine if it is reasonable with relation to <expires>.)
9. Onset Date/Time <onset>: This is an optional DateTime element that sets a specific expected begin time for the subject <event> in the <info> element. This differs from <effective> above in that <onset> refers to the beginning of the actual event that has or will take place while <effective> refers to the time that the warning about the event becomes effective. If omitted, <onset> is assumed to be the same as <sent>. The <onset> element should be used for two reasons. If there is intent to warn now about something expected to happen later on, use <onset>. If there are multiple <info> elements in the message, and the event warned of in each <info> element is expected to begin at a different time, use <onset> for the different start time in each <info> element. At the basic CAP level, IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema.
10. Expiration Date/Time <expires>: This is an optional DateTime element that sets the expiry time for all information found in the <info> element of the alert message. IT IS STRONGLY SUGGESTED THAT ALERT ORIGINATION SOFTWARE REQUIRE THIS ELEMENT or at least default it to a reasonable time after <sent> such that the user would have to deliberately force no expiry time on the message if that is what is wanted. Where there are multiple <info> elements in the same alert message, each can have its own <expires> value. IPAWS-OPEN uses <expires> in processing for queries and for choosing messages to push to IPAWS dissemination gateways. If a message has no <expires> value, IPAWS-OPEN will maintain the message as posted, but will treat the message as expired after a period of 24 hours from the value of <sent>.
11. Sender Name <senderName>: This is an optional text element for identifying the “human readable name of the agency or authority issuing the alert.” Sometimes confused with <sender>, <senderName> is the element for indicating that the creator of the alert was “XYZ County Emergency Management” or “John Doe” or both (since it is a free text field). On the other hand <sender> should be a token with no spaces that provide a machine-readable identifier (preferably associated with <senderName>). At the basic CAP level, IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema. Developers are encouraged, however to use <senderName> as it has particular value for EAS Broadcast Messages.
12. Headline <headline>: an optional text element providing a “brief, human-readable headline.” In most CAP origination software, headline creation SHOULD NOT BE OPTIONAL. The specification says that “some displays (for example short messaging service devices) may only present this headline; it SHOULD be as direct and actionable

as possible while remaining short.” Think of it this way: If you had to send the entire alert out as a Tweet (i.e., via twitter.com), what would you say? The point is that `<headline>` is used best as the short description of an alert in a list of alerts in user software and/or as the feed to short message style social media outlets. So, it should almost never be blank. (An exception might be where the alert messages are meant to be machine-to-machine with no human interaction.) IPAWS-OPEN uses `<headline>` as returned metadata in its get message list functions to allow developers to build pick lists of available messages.

13. Event Description `<description>`: This is an optional text element providing “an extended human readable description of the hazard or event that occasioned this message.” Like `<headline>`, in most CAP origination software, `<description>` creation SHOULD NOT BE OPTIONAL. It is the core (along with `<instruction>`) of what the ultimate consumer of the alert message will see and hear over whatever media is used to alert the public (and/or other members of the emergency response community). At the basic CAP level, IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema. This element is used directly, however, in IPAWS Profile messages for EAS and NWEM. Details are provided in sections below as appropriate.
14. Instructions `<instruction>`: This is an optional text element “describing the recommended action to be taken by recipients of the alert message.” This is the call to action. It describes what people should do because of the `<event>` as explained in the `<description>`. Developers may want to build a selectable, but editable, set of pre-defined calls to action that could go in the `<instruction>` element. Per the specification “if different instructions are intended for different recipients they should be represented by different `<info>` blocks.” At the basic CAP level, IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema. This element is used directly, however, in IPAWS Profile messages for EAS and NWEM. Details are provided in sections below as appropriate.
15. Information URL `<web>`: This is an optional element in the form of a “full, absolute URI for an HTML page or other text resource with additional reference information regarding this alert.” Depending on the system, this is a hyperlink to a web accessible page that further describes the situation related to the alert. At the basic CAP level, IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema. Still, developers must be sure that it validates as a formal URI or the whole alert will fail schema validation. This means that developers should carefully validate this field upon user entry to make sure there is no disruption of the alert creation process during an emergency.
16. Contact Info `<contact>`: This is an optional unedited text element that provides a place for “describing the contact for follow-up and confirmation of the alert message.” There is no particular formatting. This is just straight text that can be used for human-to-human interaction. It is not meant for automated processing. At the basic CAP level, IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema.

17. Parameter `<parameter>`: This is an optional, 0-to-many element for customizing CAP to be processed in particular ways by particular computer systems. This is second of three `<valueName>`, `<value>` pair elements in CAP. Again the `<valueName>` represents a domain of possible `<value>` entries. This element is NOT meant for meaningful human consumption. Rather is way to add processable values for those systems that understand a particular `<valueName>` domain, without getting in the way of other systems that do not understand the domain. Systems can simply ignore the `<parameter>` element entries that they do not understand. At the basic CAP level, IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema. The `<parameter>` element is used directly, however, in IPAWS Profile messages for EAS, NWEM, and CMAS. Details are provided in sections below as appropriate.

6.4 CAP Resource Block Data Restrictions and Suggestions

An `<info>` element may also contain 0-to-many `<resource>` elements. The word resource, in this case, does not refer to physical resources like trucks or supplies, nor does it refer to any form of financial resource. Instead, each `<resource>` element entry refers to “an additional file with supplemental information related to” the `<info>` element to which it is attached. Commonly, this additional file is an image or an audio file that is related in some way to the `<info>` element, although other kinds of files might also apply. In most cases, `<resource>` will describe and refer to the related file. It is possible, however, to actually attach the file in base 64 encoded form to the alert within the `<resource>` element. Actual attachment may have performance repercussions if the attached file is very large. Although there are exceptions, the potential for a drastic increase in file size and corresponding processing effort, should make developers leery of using actual attachment when other options are available. Because it is in the standard, IPAWS-OPEN will process all structures of CAP `<resource>` at the basic CAP level. Some restrictions will apply to messages intended for push dissemination through formal IPAWS dissemination channels (RSS, NWEM, EAS, and CMAS).

The IPAWS-OPEN requirements/suggestions for resource sub elements are as follows:

1. Description `<resourceDesc>`: If `<resource>` is used, you are required to describe it with a `<resourceDesc>` element that contains human-readable text. At the basic CAP level, IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema.
2. MIME Type `<mimeType>`: If `resource` is used, you are required to identify its mime-type so that machine processing of the content can occur where needed. When done correctly, the `<mimeType>` element lets an interoperating system understand the coding of the resource content such that it can determine whether it understands the content and can decode it for further use or not. At the basic CAP level, IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema. The `<mimeType>` element is used directly, however, in IPAWS Profile messages for EAS and NWEM. Details are provided in sections below as appropriate.

3. File Size <size>: This is an optional integer element indicating the approximate size of the resource file in bytes. There are two ways to handle a resource in CAP: by reference using the <uri> element and by inclusion using the <drefuri> element. When using the “by reference” technique, it is helpful to let the interoperating system know the size of the object that is being referenced, so it can decide if, when, and how to go after the file of reference. If the “inclusion” technique has been used, the <size> element is unnecessary since the file is already there as part of the message. At the basic CAP level, IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema.
4. URI <uri>: This is an optional element that provides “the identifier of the hyperlink for the resource file.” This should generally be a full and absolute URL that can be used to retrieve the referenced file from the Internet. In the event that <drefuri> is present (inclusion technique employed) the <uri> element can be used to provide a relative URI to give a name to the content of the <drefuri> element. The <uri> element in CAP is a very important element that is often confused with the previously discussed <web> element. Here is the distinction. The <web> element should be a link to a **web page** that can be browsed like any other page on the Internet to provide amplifying information on the alert. On the other hand, the <uri> element provides a direct link to a **downloadable file** that can be processed as part of the alert. At the basic CAP level, IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema. The <uri> element will, however, be used in PAWS to provide links to resources that are impractical for inclusion in an IPAWS CAP message. Details are provided in sections below as appropriate.
5. Dereferenced URI <drefUri>: This is an optional element that allows the actual inclusion of the resource file as base-64 encoded data within the CAP message. It is likely that base-64 encoded data will dramatically increase file size. So, if you use <drefuri>, you must ensure that downstream partners in any push network are capable of handling the file correctly and that partners who might poll the message from you have the understanding that message size may be quite large. The benefit of using <drefuri> to include file content such as pictures, voice, or video is that it removes the need to go back to a separate source location to retrieve needed content. This may be very important in a broadcast only situation. The disadvantage is, of course, file size; particularly on low-bandwidth networks. IPAWS-OPEN is designed to accept <drefuri> content for CAP messages at the base level. There are restrictions regarding its use in the various IPAWS dissemination channels. Details are provided in the sections below.
6. Digest <digest>: This is an optional element designed to allow use of Secure Hash Algorithm (SHA-1) to ensure that the file located at <uri> has not been changed or tampered with since the CAP message was created. Including digest in a CAP message makes it possible for connecting system to be assured that the file they retrieve by going to the <uri> location is, in fact, the file that was meant to be exposed by the original CAP message. They must, of course, be able to process the hash to do so. IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema.

6.5 CAP Area Block Data Restrictions and Suggestions

The `<area>` element is an optional 0-to-many structure that contains the geographic area to be warned. It may contain 0 or more instances of `<polygon>`, `<circle>`, and/or `<geocode>`. The area to be warned is considered to be the union of all geographic elements within the `<area>` element. By default, it should be included in all CAP messages of `<msgType>` equal to “Alert” or “Update.” This is because a good geographic description is the most effective tool for avoiding “alert spam,” where people are subjected to receiving alerts that have no interest to them. For that reason, `<area>` is required for IPAWS-Profile Alerts and all IPAWS-OPEN connected dissemination channels where push dissemination is provided. IPAWS-OPEN will accept CAP messages for retrieval without the `<area>` element in an included `<info>` element, but will not re-disseminate these messages for broadcast dissemination. Specific rules concerning `<area>` for IPAWS dissemination channels are described in sections below that describe the particular dissemination channel.

1. Area Description `<areaDesc>`: If `<area>` is used `<areaDesc>` is a required human-readable “test description of the affected area.” IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema.
2. Area Polygon `<polygon>`: The `<polygon>` element is an optional 0-to-many element within the `<area>` element that is defined in the spec as “the paired values of points defining a polygon that delineates the affected area of the alert message.” A point in the `<polygon>` consists of a decimal (WGS-84) latitude longitude value pair separated by a comma. Each pair in the sequence is separated by a space. The first and last point must be the same. A minimum of four pairs is required (which, because of the requirement for first and last pair equality, would define a triangular warning area). While there is no stated maximum, developers should be warned that there are practical maximums in the sense of excessive message length and the difficulty in decoding long strings of points. For example, using a `<polygon>` instead of a `<geocode>` to represent the State of Maryland would be kind of foolish. Here is an example of a well-formed polygon from the CAP spec:

```
<polygon>38.47,-120.14 38.34,-119.95 38.52,-119.74 38.62,-119.89 38.47,-120.14</polygon>
```

It provides a four point (five pair) parallelogram that would be useful for defining a warning area bounding box on a map. Because the formal CAP schema identifies the `<polygon>` element as a string, IPAWS-OPEN does not do additional validation for its basic CAP functionality. So, it is possible to post (and therefore also retrieve) an improperly formed `<polygon>` using IPAWS-OPEN. Applications must take special care to check the values prior to posting and after retrieval in any case where calculation based upon `<polygon>` is required. (Note: this may change going forward as IPAWS-OPEN adds internal use of `<polygon>` values. At some point additional `<polygon>` related validation code may be added.)

3. Area Circle `<circle>`: The circle element is an optional 0-to-many element within the `<area>` element that is defined in the spec as “the paired values of a point and radius delineating the affected area of the alert message.” The center of the `<circle>` consists of a decimal (WGS-84) latitude longitude value pair separated by a comma. It is followed

by a space and a radius numeric value representing the radius of the circle in kilometers. To indicate a specific point in CAP, the radius may be set to zero. In general CAP `<circle>` elements are used to define impact points and/or areas around the central point of a problem that require warning. A sample circle might look as follows:

```
<circle>38.47,-120.14 1.5</circle>
```

It would indicate that an area 1.5 kilometers in diameter around the identified point is the affected area of the situation described in the `<info>` element that contains its surrounding `<area>` element. Because the formal CAP schema identifies the `<circle>` element as a string, IPAWS-OPEN does not do additional validation for its basic CAP functionality. So, it is possible to post (and therefore also retrieve) an improperly formed `<circle>` using IPAWS-OPEN. Applications must special care to check the values prior to posting and after retrieval in any case where calculation based upon `<circle>` is required. (Note: this may change going forward as IPAWS-OPEN adds internal use of `<circle>` values. At some point additional `<circle>` related validation code may be added.)

4. Area Geocode `<geocode>`: The `<geocode>` element is an optional, 0-to-many element for identifying named, coded, and/or numbered geographic areas. It provides the capability to use a geographic code to delineate “the affected area of the alert message.” This is the third of three `<valueName>`, `<value>` pair elements in CAP. Again the `<valueName>` represents a domain of possible `<value>` entries (e.g., FIPS, SAME (for FIPS6), ZIP, STATE, etc.), while the `<value>` contains the actual code (e.g. “22406” for `<value>` with `<valueName>` equal to “ZIP”). At the basic CAP level, IPAWS-OPEN does not use this element for processing nor does it validate the internal content structure beyond what is already enforced by the schema. However certain aspects of IPAWS dissemination (EAS, NWEM, and CMAS) use this element extensively. Details will be provided in the following sections where they apply.
5. Altitude `<altitude>`: This is an optional decimal element that can prescribe “the specific or minimum altitude of the affected area of the alert message.” Interestingly, although a `<circle>` diameter is to be specified in kilometers, `<altitude>` is to be specified in feet above mean sea level. So, mixed distance measurement representation is actually specified in the CAP standard.
6. Ceiling `<ceiling>`: This is an optional decimal element that can prescribe “the maximum altitude of the affected area of the alert message.” If used, there must be a corresponding `<altitude>` element that identifies the minimum altitude. This element must also use feet above mean seal level as its measurement representation.

6.6 CAP Message Level Digital Signatures

CAP 1.2 messages may be signed at the message level (have an Enveloped Signature). For IPAWS-OPEN this is in addition to the SOAP level signature required to access the IPAWS-OPEN post and retrieval capabilities. The signature must follow the XML-Signature and Syntax processing [XMLSIG] standard. At the basic CAP level, IPAWS-OPEN does not use or validate this signature beyond what is already enforced by the schema. User system on the receiving end can choose to verify signatures that they understand as appropriate for their needs. IPAWS-

OPEN will maintain the entire message, in tact, for that purpose, but does not require the message level signature for Basic CAP exchange.

6.7 Using IPAWS-OPEN for Basic CAP Exchange

By meeting the requirements above, you can build a system that is able to exchange CAP messages with other systems using IPAWS-OPEN as a simple message broker. You can post to COGs and retrieve messages posted for your retrieval using polling techniques and query mechanisms as define in the IPAWS-OPEN Guidance document. You can keep the exchange at this level by deliberately not using the `<code>` element marker to designate the message for formal IPAWS dissemination.

7 IPAWS Profile Validation and Processing

This section describes additional requirements and suggestions that apply to message that are identified as conforming to the IPAWS profile. This information is additive to that in Section 6 above and apply to any message indented for public consumption via any of the various IPAWS push capabilities.

7.1 IPAWS Profile Validation Requirements

To identify a CAP message for formal IPAWS dissemination it must be marked and validated as an IPAWS Profile message. This means it must be validated as conforming to the Common Alerting Protocol, v.1.2 USA Integrated Public Alert and Warning System Profile Version 1.0, Committee Specification 01, 13 October 2009; known more simply as the IPAWS Profile for CAP. The following are requirements that make a regular CAP message also qualify as an IPAWS Profile message:

1. Message Status `<status>`: The `<status>` element must be equal to “Actual” for messages intended for public distribution. No message without a value of “Actual” will be disseminated to the public as an IPAWS message. This even applies to test messages intended for delivery to the public. Note that the value of “Actual” does not guarantee delivery to the public. Other restrictions may apply. But, it is a prerequisite.
2. Handling Code `<code>`: There must be one `<code>` element in the message that looks exactly like the following:

```
<code>IPAWSv1.0</code>
```

There may be other instances of `<code>` as well, but the example shown in this paragraph is the one and only marker that causes IPAWS-OPEN (and other systems) to apply IPAWS related rules to the CAP message and to consider the message for push delivery to IPAWS dissemination channels. If an “IPAWSv1.0” `<code>` value is not in the CAP message, IPAWS-OPEN will treat the message as a regular CAP message. It will not be evaluated for IPAWS specific processing.

3. Scope `<scope>`: The `<scope>` element is not mentioned directly in the IPAWS Profile, but the section concerning `<info>` elements states that “all `<info>` blocks SHALL be appropriate for immediate public release.” As a public alerting system, IPAWS will only consider CAP messages with a `<scope>` equal to “Public” as eligible for push to formal IPAWS distribution channels. Messages with `<scope>` equal to “Restricted” or “Private” will be treated as regular CAP messages and will not be further evaluated for IPAWS specific processing.
4. Reference IDs `<references>`: The `<references>` element will be checked and used to determine if messages with `<msgType>` equal to “Update” or “Cancel” have not yet expired. Messages that have invalid reference values or that refer to expired previous messages will not be disseminated over IPAWS push dissemination channels. They will

be maintained in IPAWS-OPEN and can be retrieved by systems that have proper authorization.

5. Info Block <info>: Per the IPAWS Profile, “All <info> blocks in a single alert MUST relate to a single incident or update, with the same <category> and <eventCode> values.” The point here is that you should not try to stuff what amounts to multiple kinds of alerts into the same alert message. It should be a single alert for a single purpose, not a combined alert message with each info block being used for a differing (even if related) event and/or alert purpose (<category>). Multiple <info> blocks are to be generally used only for multiple languages with the express caveat that exchange partners receiving an IPAWS profile message “may elect to process only the first <info> block encountered in a language that they support.” If multiple <info> blocks are encountered by IPAWS-OPEN in a posted message, the entire message will be maintained for retrieval. How that message is translated for push to IPAWS dissemination channels depends upon the particular rules for those channels (see later sections on EAS, NWEM and CMAS).
6. Event Code <eventCode>: At least one instance of <eventCode> is required. In particular, the IPAWS profile says “Messages intended for EAS, CMAS, and HazCollect dissemination MUST include one and only one instance of <eventCode> with a <valueName> of “SAME” and using a SAME-standard three letter <value>.” Other <eventCode> elements may be present in addition to the one SAME <eventCode>. What this means for IPAWS-OPEN is that IPAWS-OPEN will process the first <value> of the first <eventCode> with a <valueName> equal to “SAME” that it encounters. All other <eventCode> entries will be maintained in the message but will not be used to apply IPAWS Processing rules.

Also of particular note from the IPAWS Profile: “All values for EAS Event Code SHALL be passed through to 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 rule applies to dissemination devices. Individual Alerting Authorities may be restricted to the use of particular <eventCodes> in the permissions process. This restrictive capability HAS NOT been implemented in IPAWS-OPEN at this time. It is a future possibility. There are, however, some additional <eventCode> related rules that apply to particular IPAWS dissemination channels. These rules are defined in sections below (also see Appendix A).

7. Effective Date/Time <effective> and Onset Date/Time <onset>: Both <effective> and <onset> are ignored by rule if they are found in an IPAWS Profile message. The act of issuing the message is assumed to define both onset and effective time for an IPAWS Profile message. This means that the value of <sent> is the critical “start time” element in an IPAWS message. It must be effective when you send it. It must not have a future onset or effective time. If some sort of information describing future events is warranted, it can be described in the <description> or <instruction> elements as appropriate.
8. Expiration Date/Time <expires>: All IPAWS Profile conforming message MUST explicitly contain an <expires> DateTime element. IPAWS-OPEN will not process any CAP message without an explicit expires value for dissemination through formal IPAWS dissemination channels. A suggestion for developers: There are some legacy dissemination systems that require the expiry time to be defined as one of a set of

duration values from <sent>. Assuming you allow <sent> to be auto-created as you post the message, <expires> should also be auto created based on a duration selected by the user. The user should, of course be able to override this feature, but then you may have to check that the time interval between <sent> and <expires> meets the criteria set by the legacy dissemination system (see NWEM below).

9. Event Description <description>: Per the IPAWS Profile Spec: “Messages should have meaningful values for the <description>. The content in <description> may be truncated and therefore it is recommended that essential information be addressed first.” Remember, <description> is used to describe the event that has or is taking place and that <instruction> is used for a call to action for message recipients.
10. Instructions <instruction>: Per the IPAWS Profile Spec: “Messages should have meaningful values for the <instruction>. The content in <instruction> may be truncated and therefore it is recommended that essential information be addressed first.” Remember, <description> is used to describe the event that has or is taking place and that <instruction> is used for a call to action for message recipients.
11. Parameter <parameter>: The CAP specification allows the use of 0-to-many instances of the <parameter> element in a CAP message. Although other parameter instances may also exist in an IPAWS Profile conformant message, the IPAWS Profile formally addresses how three particular <parameter> instances may be built:
 - a. Messages intended for EAS and/or HazCollect dissemination MUST include an instance of <parameter> with a <valueName> of “EAS-ORG” with a value of the originator’s SAME organization code.” The suggested allowable values are “EAS”, “CIV”, “WXR”, or “PEP.” These values are only “suggested” because IPAWS-OPEN does not enforce any particular enumerated list. Other values can be used, if needed, for local purposes. A message without the EAS-ORG <parameter> still qualifies as IPAWS Profile conformant, but does not qualify for EAS Broadcast nor does it qualify for Broadcast over NOAA Radio. Without this <parameter>, IPAWS-OPEN will not distribute IPAWS Profile Messages to EAS or NWEM gateways, even if all other content would allow them to qualify (although they could be processed for a CMAS gateway). This means that, if an originator were to want an alert to go to CMAS without also going to EAS or HazCollect (NOAA Radio), he could create a message that is otherwise IPAWS Profile conformant (and conformant to the CMAS rule set as described below), but without the “EAS-ORG” <parameter>. Developers may want to include this possibility in their message origination code.
 - b. “Messages invoking the “Gubernatorial Must-Carry” rule MUST include a <parameter> with a <valueName> of “EAS_Must_Carry” and a <value> of “TRUE” for gubernatorial alerts.” IPAWS-OPEN does not do any validation on this particular rule. It is left to the disseminators and the various states.
 - c. “Messages intended for CMAS dissemination MAY include an instance of <parameter> with a <valueName> of “CMAMtext” and a <value> containing free-form text limited in length to 90 English characters.” Currently IPAWS-OPEN does not use this value in creating messages for CMAS Broadcast.

Cellular providers have defined a particular formula for building a CMAS message from a CAP message. That formula is found in Section 8.4.2 below on CMAS requirements. It is possible that a CMAMtext <parameter> could eventually be used to override that formula. This would require specific approval by the cellular industry. That is not the case today.

12. Resource Block <resource>: A <resource> element contain in the <info> element of an IPAWS Profile message offers the ability to use either pre-recorded or streaming audio or video as a broadcast source. It should be noted that the specification also says that “EAS Broadcast audio and video should match the messages textual content.” For this reason, use of the <resource> element is not formally required for IPAWS Profile conformance. In particular, it is optional for originators because disseminators are assumed to be able to provide text-to-speech capabilities for broadcast. Disseminators, however, should be prepared to handle the receipt of a properly identified resource element if it is contained within an IPAWS profile message. To make this easier, the IPAWS Profile adds some specific rules that must be applied to <resource> element contents when a <resource> element is included in an <info> element within an IPAWS Profile conformant message:

- a. Description <resourceDesc>: The following specific value for <resourceDesc> is required:

`<resourceDesc>EAS Broadcast Content</resourceDesc>`

The value is case sensitive and used exactly as shown above. Any number of <resource> elements (zero-to-many) may be used in an IPAWS Profile Message, but only the first <resource> in a chosen <info> block (see rules above) where the <resourceDesc> is an exact match and the referenced file is understood by the receiving device should be used for actual broadcast content. Note that IPAWS-OPEN does not do any actual broadcasting, so it does not try to specifically enforce this rule. It will provide the message, as submitted, to the broadcast entity where the rule will be applied. This does not apply where IPAWS-OPEN is required to do a translation from CAP 1.2 to any other format. In such cases, IPAWS-OPEN may apply the rule as stated above.

- b. MIME Type <mimeType>: The IPAWS Profile prescribes a selection of exactly four mime-types that can be used in the <mimeType> element for <resource> elements with <resourceDesc> = “EAS Broadcast Content”:
 - i. “audio/x-ipaws-audio”
 - ii. “audio/x-ipaws-streaming-audio”
 - iii. “video/x-ipaws-video”
 - iv. “video/x-ipaws-streaming-video”

No other mime-types apply for IPAWS Profile processing. The actual encoding used (e.g. mp3, etc.) is not specified in the profile specification. At This point IPAWS-OPEN does not enforce this rule on messages it receives for processing. It will provide the message, as submitted, to the broadcast entity where the rule will be applied. This does not apply where IPAWS-OPEN is required to do a

translation from CAP 1.2 to any other format. In such cases, IPAWS-OPEN may apply the rule in creating the translated result.

- c. Developers should also be aware that the specification specifically warns that broadcasters may truncate any broadcast data that exceeds two minutes in length, except for Presidential messages. Because IPAWS-OPEN is not a broadcaster, it does not enforce this limitation internally so long as the message can remain in its original CAP 1.2 format. IPAWS-OPEN may choose to enforce this rule where translation to any format other than CAP 1.2 is required. In such cases the enforcement will be on the translated result, not on the original message in CAP 1.2 format.

13. Area <area>: An IPAWS Profile conformant message requires that at least one <area> element be present. The <area> element should contain a minimum of one <geocode> element (it can include many) with a <valueName> equal to “SAME” and a <value> of “SAME” 6-digit location (also known as extended FIPS). A SAME <value> of “000000” is separately and specially defined to include ALL United States territory or territories. Per the specification, if downstream applications need to use the 5-digit FIPS code, they should do so by removing the first digit from the 6-digit extended FIPS.

The usage of <polygon> and <circle> elements is encouraged in the same area element as the <geocode> instances because they provide a “more precise geospatial representation of the area.” (Note: It appears that the IPAWS Profile spec is in conflict with the CAP spec here. CAP calls for the union of all <area> element as the warning area. The Profile is calling for polygons/circle as a refinement of the more grossly defined <geocode>.)

7.2 IPAWS-OPEN Processing of IPAWS Profile Identified Messages

When IPAWS-OPEN receives a posted CAP 1.2 message that validates to the CAP 1.2 schema, it checks to see if it is marked as an IPAWS profile CAP message. If the message is not marked, but meets all enforced regular CAP requirements, the message is saved in the IPAWS-OPEN database for retrieval as a regular CAP message. If it is marked as IPAWS Profile conformant, IPAWS-OPEN also processes all of the IPAWS Profile rules applicable in its message brokering role as listed immediately above. If the message fails, a response is returned to the sending system that provides a reason for the rejection. If it succeeds, the message is recorded in the IPAWS-OPEN database for retrieval as a regular CAP message and as an IPAWS profile conformant message.

It is then checked to see if it also qualifies for downstream push processing through formal IPAWS dissemination channels.

8 IPAWS Dissemination Channel Processing

This section describes the data instance requirements and validation process that causes an IPAWS profile conformant message to actually be pushed out on IPAWS through IPAWS dissemination channels. These channels include EAS Broadcast (radio and TV), NOAA Weather Radio for Non-Weather Emergency Messages (NWEM), and Cellular Mobile Alerting Services (CMAS).

8.1 Digital Signatures (again)

The IPAWS profile conformant message is then checked to see if it has the optional message-level digital signature as defined in the CAP 1.2 specification, and, if it does, whether IPAWS-OPEN can validate the signature. IPAWS Conformant message without message level signatures, or with signatures that cannot be validated by IPAWS are recorded for retrieval by authorized systems with access to IPAWS-OPEN but are not “pushed” to formal IPAWS Dissemination gateways, regardless of content conformance. Messages with validated signatures are made available to the public RSS feed and are further processed to determine compatibility with EAS, NWEM, and CMAS Gateway requirements.

8.2 EAS Requirements

Messages meeting the IPAWS Profile and EAS requirements will automatically be provided to broadcasters for transmission to the public in all geographic areas denoted in the <area> block of the CAP message as defined in FCC rules.

8.2.1 EAS Data Restrictions and Suggestions

Messages for broadcast over radio and TV stations are most often translated from CAP to EAS Decoder specifications found in FCC rules under CFR Part 11.33. Because this is done downstream from IPAWS-OPEN and because the “ECIG Recommendations for a CAP EAS Implementation Guide” document covers this process in some detail it will not be repeated here. But, a proper EAS message does require certain things from its upstream CAP message. Because IPAWS-OPEN is focused on the CAP message, this section will cover those requirements and how IPAWS-OPEN does, or does not, validate those requirements before pushing the CAP message to EAS Gateways. In general, the requirements for the IPAWS Profile (section 6 above) are the requirements for EAS and IPAWS-OPEN will attempt to push any IPAWS Profile message to its EAS Gateways. How they are handled by each gateway may depend upon content as identified here. (Note that this section will also be defined element by element. When an element is omitted here, the regular rules for the IPAWS Profile apply with no added information required.)

1. Message Type <msgType>: Any message containing a <msgType> element other than “Alert” or “Update” or “Cancel” will be ignored by EAS dissemination devices.

2. Info Block <info>: Per the ECIG Recommendation for CAP Implementation Guide: “At least one <info> block is required for translation into EAS. A special Case is <msgType> equal to “Cancel” where no <info> block is required and no translation to EAS is needed. Multiple <info> blocks may be used to encode alert information in multiple languages. If the same language is defined for multiple <info> blocks, then only the first block SHALL be processed.” Note that the <language> element within an <info> element denotes the language of the <info> element. Generally speaking, a broadcasting activity will seek an info block with the <language> it uses as a primary broadcast language. If not found, it will default to English.
3. Event Type <event>: A required CAP field, but not employed in the translated EAS message. For EAS is should generally be an Event Name corresponding to Event Code <eventCode> as listed in Appendix A.
4. Urgency <urgency>: A required field that should be set to “Unknown” by the originator for all test alerts (<eventcode>.<valuename> = SAME and <eventCode>.<value> = RWT, RMT, NPT, DMO, and NMN).
5. Severity <severity>: A required field that should be set to “Minor” by the originator for all test alerts (<eventcode>.<valuename> = SAME and <eventCode>.<value> = RWT, RMT, NPT, DMO, and NMN).
6. Certainty <certainty>: A required field that should be set to “Unknown” by the originator for all test alerts (<eventcode>.<valuename> = SAME and <eventCode>.<value> = RWT, RMT, NPT, DMO, and NMN).
7. Event Code <eventCode>: Not all EAS dissemination devices will handle all possible event codes although they should handle all FCC defined EAS Codes. Unknown codes will cause the message to be ignored by the dissemination device. IPAWS-OPEN will not enforce the content of the SAME based <eventCode>. It will enforce the structure as a three letter, all CAPs value.
8. Expiration Date/Time <expires>: The <expires> element is required and “used to derive EAS Valid Time Period (TTTT) by subtracting from <sent> to derive a duration, round resulting duration of two next valid EAS Duration length. EAS duration range: if greater than zero and less than or equal to 45 minutes, ‘15, 30, 45 min.’ else every half hour from one hour to 99 hours 30 min. If duration is less than or equal to zero, or the message is expired, it SHALL be ignored.” What this means for developers is that they can put in whatever time stamp they want for expires and the EAS disseminator will round to the appropriate interval for EAS. If the expires time is earlier than the sent time or has already been passed by the current clock time the disseminator will ignore the message.
9. Sender Name <senderName>: The <senderName> element is an optional text element for identifying the “human readable name of the agency or authority issuing the alert. This is the element for indicating that the creator of the alert was “XYZ County Emergency Management” or “John Doe” or both (since it is a free text field). EAS Dissemination devices will use this element in conjunction with description and instruction to actually construct the alert text or other visual display for an EAS message.

For this reason, although it is technically optional, `<senderName>` is an important element in the construction of a proper EAS message.

10. **Headline `<headline>`:** The ECIG recommendation suggests not using this element in construction of text or other visual display. The `<headline>` element, however, is the appropriate element to use for the entire message that may be sent as a short message text as in SMS messaging or via Twitter. It should be noted, however, that `<headline>` will not be used for actual EAS broadcast.
11. **Event Description `<description>`:** The ECIG recommendation suggests using `<description>` in between `<senderName>` and `<instruction>` in creating EAS alert text or other visual displays. A `<description>` describes the event that has taken place, or will take place, but does not include the call to action by the recipient of the message. Be aware that the combined length of the words “Message from: “ plus `<senderName>`, `<description>`, and `<instruction>` must be less than 1800 characters or some form of truncation may occur. If a `<description>` must be detailed for other CAP usage, the most important facts should be at the beginning so that they are not truncated.
12. **Instructions `<instruction>`:** The ECIG recommendation suggests using `<instruction>` after `<description>` in the creation of an EAS alert text or other visual display. Developers should remember that `<instruction>` is designed for the formal call to action for message recipients. As such this field may be something that can be built from a pick list, although it should also be editable by the user. Be aware that the combined length of the words “Message from: “ plus `<senderName>`, `<description>`, and `<instruction>` must be less than 1800 characters or some form of truncation may occur. If an `<instruction>` must be detailed for other CAP usage, the most important call to action should be at the beginning so that it is not truncated.
13. **Parameter `<parameter>`:** The ECIG recommendation adds an optional “EASText” parameter `<valueName>` to what is identified in the IPAWS Profile. The `<value>` would be the actual text desired for broadcast and within the 1800 character limitation for the text portion of an EAS message (similar to “CMAMText” for CMAS). This suggestion is not endorsed by IPAWS because it creates a situation where the broadcast text for EASText and the actual warning (combination of `<description>` and `<instruction>`) could differ significantly. Instead, the IPAWS Program endorses the truncation method defined in the ECIG recommendation if the combined text entries used from a CAP message are found to exceed the 1800 character limitation for EAS broadcast. “EASText,” like any other externally defined parameter, will be maintained from the originator in a forwarded CAP message, but IPAWS-OPEN will perform no content review or other validation or endorsement. “EASText” is not part of the IPAWS Profile. It is merely optional CAP content per the regular CAP 1.2 specification.
14. **Resource Block `<resource>`:** The `<resource>` element may be used in EAS to provide a link to a recorded or streaming audio or video. In using resource the ECIG recommendation suggests that `<derefuri>` not be used. Accordingly, any `<resource>` element containing `<derefuri>` may be ignored by EAS dissemination devices. The `<uri>` element is required where resource is used. The `<uri>` element must refer to an accessible URL that the disseminating system can reach. The ECIG recommendation

also limits the file formats to be used for file download to MP3 and WAV. Other file formats may not be recognized by downstream EAS dissemination devices. IPAWS-OPEN does not enforce particular file formats internally. It is important that alert origination software identify the appropriate file format as required.

15. Area Block <area>: The ECIG recommends that disseminating systems recognize only the first area block regardless of the number area blocks in the CAP message.
16. Area Description <areaDesc>: The <areaDesc> element is required in the CAP specification. It will not be used in the resulting EAS message. Originators should include pertinent area information in the description or instruction elements as needed.
17. Geocode <geocode>: Messages with no <geocode> or messages with no <geocode> elements that have a <valueName> = “SAME” will be ignored by EAS dissemination devices. Additionally, legacy limitations on the EAS format make it possible that only the first 31 valid SAME <geocode> entries will be accepted. Others may be identified, but they may not be used for actual EAS broadcast.

8.2.2 EAS Message Construction

Using the rules above allows an IPAWS Profile message to be translated by EAS Dissemination Equipment into an actual EAS Broadcast message. The specific details are beyond the scope of this document (see the ECIG Recommendation) but a general discussion is appropriate for those who build CAP alerts for IPAWS-OPEN to forward for EAS Broadcast. There are two parts of the EAS Message: Header and Content.

The header includes:

1. ORG (originator) taken from EAS-ORG in <parameter>.
2. EEE (Event code) taken from <eventCode> <value> with <valueName> = “SAME”
3. PSSCCC (Location Code) a list taken by combining all (up to the first 31) <geoCode> <value> contents where the <valueName> = “SAME”
4. TTTT (Duration) taken as the interval between <sent> and <expires> rounded to the next highest interval allowed (see <expires> above) up to 99 hours and 30 minutes.
5. JJHHMM (Time) taken from <sent>.
6. LLLLLLLL (EAS Station ID) locally assigned.

The content is either:

1. Audio and/or video as represented in resource, or
2. Text that is a combination of the phrase “Message From ” followed by senderName, description, and instruction from the original CAP message. Both description and instruction are subject to truncation if the length of the resulting string is greater than 1800 characters.

8.2.3 EAS Message Distribution Channels

{TBD – Specific Documentation of public and private RSS feeds to be implemented is underway and should be available by late June 2011 or earlier}

8.3 NWEM Requirements

Non-weather Emergency Messages (NWEM) are a specialized form of IPAWS Profile conformant message. Because the message meet the IPAWS profile they can also be sent to EAS and CMAS if the meet the combined requirements (i.e., Conform to the IPAWS Profile AND to the specialized requirements of EAS, NWEM, and CMAS).

Messages created by NOAA authorized alerting Authorities that also meet the IPAWS Profile and NWEM requirements will automatically be sent to the public via NOAA Radio broadcast as defined in NOAA regulations in all geographic areas denoted in the <area> block of the CAP message.

8.3.1 NWEM Data Restrictions and Suggestions

There are a few general restrictions on data used in an NWEM Message:

1. There are some tags that are required for CAP, but not used in NWEM. NWEM builders should use these fields appropriately as NWEM Messages may also travel on Cap networks.
2. There are some optional tags that are required for NWEM. Some of these have special content restrictions. Those restrictions are needed in order to support NOAA's downstream systems.
3. Some cardinalities are more restrictive in NWEM than they are in CAP. These cardinality restrictions are also required to adequately support downstream system requirements.
4. Finally, there are some tags that are optional in CAP and not used by HazCollect. As in item 1 above, the OPEN interface will take these fields but will not process them thorough NWEM. If the message is also posted though the general CAP network, these tags will be processed appropriately.

Specific requirements and recommendation for each element with characteristics other than what has been defined in Basic CAP and IPAWS profile are as follows:

1. Message ID <identifier>: The <identifier> element must be a unique identifier across the system. Suggest using a system identifier in form of an actual identifier string. You may use any unspaced token string that that you like, but it should carry a guarantee of uniqueness.

2. Message Status <status>: While only Messages with a <status> equal to “Actual” will be considered for push to the public by IPAWS, NWEM does allow other status for internal test purposes etc. “Actual,” “Exercise,” “System” and “Test” are allowed. “Draft” is not. The <status> element itself is not used in the actual NWEM message, but is used in pre-processing. For any message other than “Actual” the following text will *automatically be added by the HazCollect Server* to the resulting NWEM message translation: "THIS IS A <status> MESSAGE. DO NOT TAKE ACTION BASED ON THIS <status> message..." This additional text WILL NOT be added to the text of the CAP message itself. Messages broadcast on other CAP networks will need to take this into account and add specific additional warnings to the description field in the info block of the CAP message, where applicable. Such additional warnings are OK with the HazCollect system as they re-emphasize the fact that a message is not an “actual” alert.
3. Message Type <msgType>: The <msgType> element is not directly used in NWEM but is valid for NWEM messages passed in parallel through CAP channels. It is also used in NWEM pre-processing. The server will use an “Error,” “Update” or “Cancel” message to do exactly that if the message references a previously sent NWEM Alert that has not yet expired. The Error, Update or Cancel message must properly reference the originating message in its <references> element.
4. Source <source>: The <source> element is used by NWEM, in combination with the CAP <identifier> to “sign” the bottom of the message in its NWEM format. Its suggested format is Last name of sender and initials. An example is as follows:

```
<source>HamGA</source>
```

This is not the “normal” CAP way to identify a personal sender. The <senderName> element is suggested instead. However, NWEM also has a specific use for <senderName> as well. (See xx Below). It is possible that this restriction will change to a more standard usage as NWS systems evolve.

5. Scope <scope>: All NWEM Messages must have a <scope> equal to “Public.”
6. Reference IDs <references>: The <references> element is not used directly in an NWEM message but is valid for NWEM messages passed in parallel through CAP channels and is processed by the NWEM server to update unexpired previous NWEM messages. The server will use an “Error,” “Update” or “Cancel” <msgType> message to do exactly that if the message references a previously sent NWEM Alert that has not yet expired.
7. Info Block <info>: An NWEM instance can have only one <info> block vice the many allowed in regular CAP messaging. For IPAWS-OPEN this means that, if multiple <info> blocks are encountered in an IPAWS Profile conformant CAP message, only the first <info> block will be considered for NWEM Processing.
8. Language <language>: The <language> is required. Only two values allowed: “en-US” or “sp-US.” The language value should match the language of the NOAA Radio broadcast facility that is responsible for the <area> block identified in the message. (Currently, this means that “sp-US” should only be used for Puerto Rico in messages intended for NWEM distribution.)

9. Event Type <event>: The <event> element is required field for NWEM and is still a string. The specific string however is specialized from CAP. It must be one of an enumerated set of NWEM names and must relate to the Event Code tag below. For NWEM, it is the text name of the SAME Code found below in <alert><info><eventCode><value>. The allowed values are found in Appendix A below. For translation to NWEM, the <event> tag will be auto-generated from the table in Appendix C.
10. Event Code <eventCode>: EAS Rules for the <eventCode> also apply to NWEM messages. The actual list of acceptable <eventCode><value> entries will largely overlap, but are not completely the same. Originators other than NWS personnel are not normally authorized to create messages that employ specific weather warning codes. The specific list of allowed values for NWEM are found in Appendix A below.
11. Effective Date/Time <effective>: For IPAWS-OPEN the <effective> element is ignored for NWEM translation. The effective time of the message is assumed to be the same as <sent>.
12. Expiration Date/Time <expires>: As for EAS, the <expires> element is required for NWEM messaging. Known as “Product Purge Time” in the NWEM environment, it has some special requirements in terms what is value must be:
 - a. It must not exceed <sent> by more than 360 minutes.
 - b. It must differ from <sent> in exactly 15 minute intervals up to 120 minutes.
 - c. It must differ from <sent> in exactly 30 minute intervals between 120 and 360.

Because of this exactness requirement, developers should consider setting this time with a pick list of durations of duration time to be applied the <sent>. Notice that these durations are a subset of the same durations defined for EAS. When building an interface, users might appreciate how a chosen duration might affect the dissemination route of the alert message that they create. Also please note that EAS will round up to the nearest interval defined as the difference between <sent> and <expires>. NWEM requires exact values in the CAP alert and will reject (for NOAA Broadcast) messages that have an interval between <sent> and <expires> that does not calculate to an allowed duration. In the event that a client application does not implement this requirement accurately, IPAWS-OPEN will use the same “rounding up” rules that apply to EAS translation above, except that the maximum duration allowed will be 360 minutes.

13. Sender Name <senderName>: The <senderName> element is a required and specifically formatted field for NWEM in the format : <CogName>,<City>,<State>. AN example is provided as follows:

<senderName>IPAWS Interoperability COG,Stafford,VA</senderName>

The above is a rather IPAWS-OPEN specific construction of <senderName> geared to facilitate the translation of the CAP message into downstream NWEM formatting. It does not violate any generic CAP rules as to structure of <senderName> and actually enhances the use of senderName for EAS according to ECIG Guidelines by providing a predictable, coherent structure for use in building the EAS test according to those

guidelines. Developers may want to auto generate this value for their users. It may also be advisable to allow manual override of this field, with the caveat that overridden values may cause the message to be disallowed for NWEM processing if the overridden format is not correctly entered.

14. Event Description <description> and Instructions <instruction>: When IPAWS-OPEN Translates an NWEM destined CAP message for actual NWEM processing it must concatenate <description> and <instruction> into the text used for that NWEM. Further, the translation is limited to a single field that must be <= 160 words. So the description text in a broadcast NWEM includes the <description> element plus what might also be in the <instruction> field of a normal CAP message. IPAWS-OPEN concatenates the two elements for creating an NWEM message, but maintains the original structure for disseminating copies of the NWEM CAP message to other IPAWS users and networks. This allows the call to action portion of the CAP message to be properly placed within the instruction tag per the CAP specification. Developers may want to control the number of words (and or characters, based on EAS requirements above) in their user creation interfaces. They may want to allow users to override these limits with the caveat that they risk truncation (EAS) or rejection (NWEM) if limits are exceeded, but also that other dissemination methods would not be affected.
15. Area Block <area>: Previous (for CAP 1.1) instructions stated that “each FIPS, ZONE, or STATE CODE gets it own <area> block in a NWEM Message.” With CAP 1.2, it is required that FIPS and Zone Codes be put into a single <area> block for processing.
16. Area Description <areaDesc>: The <areaDesc> tag should contain the administrative name (or names) corresponding to the <geocode> entries included in the <area> block. These names (along with all geocode values authorized to a particular COG for NOAA Radio Broadcast) can be retrieved from IPAWS-OPEN programmatically using the getNWEMAuxData function (See IPAWS-OPEN Programmers Guidance). IPAWS-OPEN will not validate this field beyond normal schema validation. It is also not used directly by NWEM on the NOAA HazCollect Server. (They use their own look-up of the code to identify county and marine zone names).
17. Area Polygon <polygon> and Area Circle <circle>: The current implementation of HazCollect at NWS does not use <polygon> or <circle> within <area>. Support for these structures is projected for a future release.
18. Geocode <geocode>: NWEM messages use the same rules for the <geocode> element as EAS as a begin point, but there are some differences:
 - a. NWEM uses only the last five digits of the SAME location code (found in the <value> of a <geocode> with <valueName equal to “SAME”) for its actual broadcast decision-making. This is equivalent to the 5 digit FIPS code for U. S. counties and independent cities. It strips off the first number to find the FIPS 5 equivalent. Resulting duplicates are ignored.
 - b. NWEM also recognizes <geocode> entries with <valueName> equal to “ZONE.” These are National Weather Service managed Marines Zones representing U.S. contiguous waters for which warning may be applicable.

- c. Each particular COG in IPAWS is authorized 0 or more 5-digit FIPS codes and 6 digit ZONE codes to which the authorized COG is allowed to broadcast. These values are dynamically retrievable through IPAWS-OPEN using the getNWEMAuxData function (See IPAWS-OPEN Programmers Guidance). Developers will want to make this call in their software in order to populate pick lists for users to select from when creating alerts for NOAA Radio Broadcast. The five digit FIPS must be turned into 6 digit SAME codes prior to populating the actual alert. Prefixing a code with zero will allow EAS and NOAA Radio (and possible CMAS) broadcast to the entire county. Prefixing the code with 1 through 9 will prescribe EAS and CMAS to the smaller area within a county corresponding to the 6-digit SAME code.

8.3.2 NWEM Authorization and Training Requirements (Developer's Viewpoint)

TBD

8.3.3 NWEM Message Distribution Channels

TBD

8.4 CMAS Requirements

This section describes CAP data requirements from the perspective of translation to the CMAC Standard (Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification, J-STD-101 approved October 2009). Among other things, this 126 page standard describes what it requires from a CAP message to make it possible for IPAWS-OPEN to push alerts to Cellular Mobile Service Provider (CMSP) Gateways for broadcast to cell phones based on the location of the cell phone itself in relation to the <area> block defined in the message. A distillation of those requirements is provided in Sections 8.4.1 and 8.4.2 below.

8.4.1 CMAS Data Restrictions and Suggestions

As a start, a CMAS message must, of course validate to the IPAWS Profile (per Section 7 above). It also must contain no URLs or telephone numbers in elements translated for CMAS use. An exception is allowed for telephone numbers in Child Abduction Emergencies ((<eventCode><value> equal to "CAE") and for both URLs and telephone numbers in Presidential Alerts (<eventCode><value> equal to "EAN"). Beyond that, there are certain values that must be found in an IPAWS Profile conformant CAP messages to ensure that it will be treated as a CMAS message. Those values are described as follows:

1. Message Type <msgType>: This required field must contain one (of many) specific values; please see CAP v1.2 standard for allowed values. Only messages with <alertType> equal to “Alert”, “Update,” or “Cancel” will be passed to CMSP Gateways.
2. Severity <severity>: This required field must contain one (of several) specific values; please see CAP v1.2 standard for allowed values. Only messages with <severity> equal to “Extreme” or “Severe” will be passed to CMSP Gateways. This restriction does not apply to presidential and child abduction alert messages (<eventCode> <value> element equal to “EAN” or “CAE”).
3. Urgency <urgency>: This required field must contain one (of several) specific values; please see CAP v1.2 standard for allowed values. Only messages with <urgency> equal to “Immediate” or “Expected” will be passed to CMSP Gateways. This restriction does not apply to presidential and child abduction alert messages (<eventCode> <value> element equal to “EAN” or “CAE”).
4. Certainty <certainty>: This required field must contain one (of several) specific values; please see CAP v1.2 standard for allowed values. Only messages with <certainty> equal to “Observed” or “Likely” will be passed to CMSP Gateways. This restriction does not apply to presidential and child abduction alert messages (<eventCode> <value> element equal to “EAN” or “CAE”).
5. Expiration Date/Time <expires>: As is true for EAS, the <expires> element is required for CMAS messaging. The limit to duration (the time between <sent> and <expires> is limited to 24 hours. This is a shorter duration than either EAS or NWEM. Messages that have already reached the <expires> DateTime, or where the difference between <sent and <expires> exceeds 24 hours, will not be passed to CMSP gateways.
6. Language <language>: Currently, only English (“en-US”) is supported for CMAS. If no <info> block with <language> equal to “en-US” is found in an IPAWS Profile message, that message will not be passed to CMSP gateways.
7. Area Polygon <polygon>: An IPAWS conformant CAP message will be rejected for CMAS transmission if it has a <polygon> element that includes more than 100 points.

8.4.2 CMAS Message construction

The actual CMAS message that will be broadcast to cell phones is limited by regulation to a maximum of 90 Characters. A particular formula is suggested for creating those 90 characters. That formula is described in Appendix A to J-STD-101. This Appendix is “informative,” meaning that the formula is not a cut-in-stone absolute. This means that IPAWS or the Cellular Provider Gateways may deviate where warranted so long as no “normative” (absolutely required) requirements from the rest of the standard are broken. In simplified form, Appendix A of J-STD-101 says to:

1. Describe what is happening: Use the text string associated with the <eventCode> <value> from the CAP message with <valueName> = “SAME.” (See Appendix A.)

2. Describe the location: Standard text of “in this area” should be sufficient for the actual message text since the alert will be broadcast only to cell phones where the connecting cell tower is within the affected area defined in <area> in the base CAP message.
3. Describe when the alert expires: Translate the value of <expires> from the base CAP message into 12 hour/Time zone format (e.g., “until 7:00AM PDT”)
4. Describe what action should be taken: Use a set of string texts associated with the combination of <responseType> and <eventCode> that make the most sense as a call to action for cell phone customers.

An alternative found in the IPAWS Profile is to use a <parameter> with <valueName> equal to “CMAMText” and a <value> equal to any string up to 90 characters that meets the gist of the message content described immediately above. In current processing, the “CMAMText” <parameter> will not actually be used to create the CMAS message. This may change as IPAWS and CMAS evolve

8.5 Amber Alert Requirements

TBD

9 Access to IPAWS-OPEN messages

Sections 4 through 8 all concerned building CAP alerts for the IPAWS-OPEN environment. This section describes access to those messages. In particular it describes data access (who can get what messages and how). For those with query access, it also describes what information can be used in query parameters and where that information comes from in either the CAP message or in other metadata.

9.1 CAP Query Metadata in IPAWS-OPEN

There are two kinds of metadata that apply to CAP messages forwarded through IPAWS-OPEN, content metadata and usage metadata. Content metadata is data gleaned from the actual content of the messages that can be used by authorized retrieval systems to retrieve the messages according to their content. Usage metadata is metadata related to where and to who the message was transmitted and/or who retrieved particular messages and when using query capabilities. Query capability in IPAWS-OPEN is based on both types of metadata. Do you have access? If you do, what data can be used to retrieve messages themselves and or other information about message usage?

9.2 Data Access Questions

There are two types of access available from IPAWS-OPEN, Feed Consumers and Query consumers. Feed consumers include:

1. Anyone with Internet access qualified for the Public RSS Feed. This feed will include all IPAS Profile Conformant CAP messages that include IPAWS validated message level signatures. It will not be filtered. Consumer systems will be responsible for filtering and using the messages to meet their users' needs. (It is possible that differentiated feeds may be developed in the future. Initially, they will not.) Valid public CAP messages that do not meet the IPAWS Profile, or that meet the IPAWS profile, but are either unsigned or are signed with signatures unrecognized by IPAWS, will not be available through this feed.
2. Any system that feeds a formal EAS Broadcast responsibility qualifies for the Private EAS CAP feed. This feed will include a subset of the Public RSS Feed because it will provide only those messages that also qualify according to the EAS Requirements in Section 7.2 above. This feed is designed to provide to easy access for Next Generation EAS Devices that support broadcasters who are required by FCC regulation to participate in EAS broadcasting.

All other access is provided by SOAP query as defined in the IPAWS-OPEN Programmers Guidance Document. SOAP query will allow greater and also more fine-grained access to all CAP messages. In particular the query capability provides:

1. Access to CAP messages posted from one COG to another COG (or COGs) using a <scope> equal to "Private" or "Restricted." Such message are, by definition, not IPAWS Profile messages, but they may be important for warnings among responder organizations

that are not ready for (or are not aimed at) “Public” consumption. In this case, retrieval by COG “X” is only available if the originating COG specified “COG =X” in the <addresses> element of the CAP message or if COG “X” member was the message originator.

2. Access to all CAP messages with <scope> equal to “Public.” This includes the messages that are on the Public RSS Feed, but also those “Public” messages that are not in IPAWS Profile (e.g., regular CAP) and those IPAWS Profile messages where the signature was absent or could not be validated by IPAWS.
3. Granular access to desired subsets of 1 and 2 above using appropriate query parameters (Section 9.3 below)

9.3 Data Content and Usage Queries

Logically, data content and usage queries in IPAWS-OPEN could be defined by any combination of three types of query parameter content. These include query using metadata based on the values found in certain elements in the CAP message itself, using geography as defined in the <area> element, and using distribution channel information. Not all of the particular functionality is in place. Some has already been implemented. Some (geographic queries in particular) have not yet been implemented. The reason for identifying all of the possibilities here is that, although there could be significant behind the scenes processing required, any combination of the three could be used in the IPAWS-OPEN getMessage or getMessageList functions as defined in the IPAWS-OPEN Programmers guidance without change to the actual interface or return data schema.

9.3.1 Basic CAP Elements used as Retrieval Metadata

Metadata elements may be combined into a query that looks for particular values of the CAP elements <identifier>, <sender>, <sent>, <status>, <msgType>, <scope>, <code>, <addresses> and <incidents>.

9.3.2 Geographic Elements used as Retrieval Metadata

Values for <geocode> <value> are also treated as metadata in the standard IPAWS query function. Note that <valueName> is ignored. The metadata used for query will be the entries of <value> within <geocode> regardless of the actual entry in the <valueName> element. The <circle> and <polygon> elements are targeted by IPAWS for eventual query use but that use has not been yet been implemented.

9.3.3 Dissemination Path Retrieval Metadata

The <scope> element, with its values of “Public”, “Private”, and “Restricted”, offers one level of dissemination information. The <code> element can also be used to identify that the alert is both “Public” and IPAWS Profile conformant. If so, the further query of the Dissemination Channels used can be made. Using the query Parameter equal to “channel” can be used with values of “RSS”, “EAS”, “NWEM”, and/or “CMAS.”

10 Summary and Suggested Course for Development of a CAP Interface

This document is designed to help developers build CAP 1.2 Message for transport via IPAWS-OPEN to other systems and to official IPAWS dissemination channels. Used properly, developers can build an interface that guides users toward building a CAP message that meets their needs with only a few simple questions:

1. Is this CAP message meant for specific addressees only? Set the <scope> element equal to “Private” and build for regular CAP.
2. Is the CAP message intended for a specific audience beyond its basic addresses but not intended for the general public? Set the <scope> element equal to <restricted> and provide and test input to provide the restriction details. Then build for regular CAP.
3. Is the CAP message allowed to go to the public, but not intended for widespread IPAWS broadcast? Set the <scope> equal to “Public” and build for regular CAP.
4. Is the message meant for IPAWS dissemination? Set the <scope> element equal to “Public” and add a <code> element equal to “IPASv1.0.” Build an IPAWS profile message.
5. As your user builds the message, identify any values entered that would disallow any of the dissemination channels, but let them choose what to actually enter as long as the IPAWS Profile itself is not violated.

The result will be a truly usable user interface. With all of the variables involved in CAP messaging and all of the different dissemination environments, building an easy to understand interface is not easy, but it is valuable. Hopefully, the information in this document will at least make it possible. Your user base will appreciate it.

11 Appendix A - Event Code Applicability by Dissemination Channel

Table 11-1 below identifies the <eventCode> element values and their corresponding description applicable for auto-populating the <event> element (or vice versa). The next four columns indicate yes or no values. The “Create in Standard Client” column identifies those event codes that a typical non-weather warning authority might be authorized to use in building alerts for IPAWS dissemination. The next three columns indicate the capability for IPAWS to actually use a message containing the identified <eventCode> for push dissemination. Client applications should be prepared to receive and process message from these dissemination sources as appropriate based on the mission of the client application. For example, a Winter Storm Warning (WSW) is obviously inappropriate for a Non Weather Emergency Message. Similarly, CMAS will not be used when the level of alert is a “Watch,” but will be used for an imminent “Warning.”

There are three special cases identified by asterisks below:

1. Child Abduction Emergencies are a particular form of CAP message (with a default translation from the NIEM Amber Alert standard which may actually be used by public safety authorities) that may be available to local alerting authorities to create, but will require review at a higher level before actual transmission via IPAWS-OPEN. Specific rules are still being developed.
2. Presidential Alerts (EAN) will not be allowed from message originators other than those in the White House itself. For that reason it is marked “N” for creation by all other originators. Systems should, however, be able to receive, and give priority to, messages with <eventType> equal to “EAN.”
3. Practice/Demo Warnings (DMO) will not be disseminated, but will be used for demonstrations of interoperability public events (e.g., the annual National Association of Broadcasters (NAB) Show or the International Association of Emergency Managers (IAEM) Convention). Vendors of all kinds may want to participate in such events. If so they should build products with the option of using <eventCode> with a value of “DMO” for such events.

Table 11-1. IPAWS Event Codes

Event Code	Event Name	Create in Standard Client	Dissemination		
			EAS	NWEM	CMAS
ADR	Administrative Message/Follow up Statement	Y	Y	Y	N
AVA	Avalanche Watch	Y	Y	Y	N
AVW	Avalanche Warning	Y	Y	Y	Y
BZW	Blizzard Warning	N	Y	N	Y
CAE	Child Abduction Emergency*	Y	Y	Y	Y

Event Code	Event Name	Create in Standard Client	Dissemination		
			EAS	NWEM	CMAS
CDW	Civil Danger Warning	Y	Y	Y	Y
CEM	Civil Emergency Message	Y	Y	Y	Y
CFA	Coastal Flood Watch	N	Y	N	N
CFW	Coastal Flood Warning	N	Y	N	Y
DMO	Practice/Demo Warning*	Y	N	N	N
DSW	Dust Storm Warning	N	Y	N	Y
EAN	Presidential Alert *	N	Y	Y	Y
EQW	Earthquake Warning	N	Y	Y	Y
EVI	Immediate Evacuation Warning	Y	Y	Y	Y
FRW	Fire Warning	Y	Y	Y	Y
FFA	Flash Flood Watch	N	Y	N	N
FFS	Flash Flood Statement	N	Y	N	N
FFW	Flash Flood Warning	N	Y	N	Y
FLA	Flood Watch	N	Y	N	N
FLS	Flood Statement	N	Y	N	N
FLW	Flood Warning	N	Y	N	Y
HMW	Hazardous Materials Warning	Y	Y	Y	Y
HWA	High Wind Watch	N	Y	N	N
HWW	High Wind Warning	N	Y	N	Y
HUA	Hurricane Watch	N	Y	N	N
HUS or HLS?	Hurricane Statement	N	Y	N	N
HUW	Hurricane Warning	N	Y	N	Y
LAE	Local Area Emergency	Y	Y	Y	N
LEW	Law Enforcement Warning	Y	Y	Y	Y
NIC	National Information Center	N	Y	Y	N
NPT	National Periodic Test	N	Y	Y	N
NUW	Nuclear Power Plant Warning	Y	Y	Y	Y

Event Code	Event Name	Create in Standard Client	Dissemination		
			EAS	NWEM	CMAS
RHW	Radiological Hazard Warning	Y	Y	Y	Y
RMT	Required Monthly Test	N	Y	Y	N
RWT	Required Weekly Test	N	Y	Y	N
SPW	Shelter In Place Warning	Y	Y	Y	Y
SMW	Special Marine Warning	N	Y	N	Y
SVA	Severe Thunderstorm Watch	N	Y	N	N
SVR	Severe Thunderstorm Warning	N	Y	N	Y
SVS	Severe Weather Statement	N	Y	N	N
TOA	Tornado Watch	N	Y	N	N
TOE	911 Telephone Outage Emergency	Y	Y	Y	N
TOR	Tornado Warning	N	Y	N	Y
TRA	Tropical Storm Watch	N	Y	N	N
TRW	Tropical Storm Warning	N	Y	N	Y
TSA	Tsunami Watch	N	Y	N	N
TSW	Tsunami Warning	N	Y	N	Y
VOW	Volcano Warning	N	Y	Y	Y
WSA	Winter Storm Watch	N	Y	N	N
WSW	Winter Storm Warning	N	Y	Y	Y

12 Appendix B - Acronyms

Acronym	Explanation
ATIS/TIA	Alliance for Telecommunications Industry Solutions/Telecommunications Industry Association
CAP	Common Alerting Protocol
CMAS	Cellular Mobile Alerting Service
CMSP	Commercial Mobile Service Provider
COG	Collaborative Operating Group
EAS	Emergency Alert Service
ECIG	EAS CAP Industry Group
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
HTML	Hypertext Markup Language
IPAWS	Integrated Public Alert and Warning System
IPAWS-OPEN	Integrated Public Alert and Warning System – Open Platform for Emergency Networks
NOAA	National Oceanic and Atmospheric Administration
NWEM	Non-Weather Emergency Message
NWS	National Weather Service
OASIS	Organization for the Advancement of Structured Information Standards
OPEN	Open Platform for Emergency Networks
RSS	Really Simple Syndication
SAME	Specific Area Message Encoding
SHA-1	Secure Hash Algorithm - 1
SOAP	Simple Object Access Protocol
URI	Universal Resource Identifier
WGS-84	World Geodetic System 1984
WS-Security	Web Services Security
XML	Extensible Markup Language
XMLSIG	XML-Signature and Syntax processing
ZIP	Zone Improvement Plan (U. S. Postal Service Code)